

GROUPS WITH NO PARAMETRIC GALOIS EXTENSION

PIERRE DÈBES

ABSTRACT. We disprove a strong form of the Regular Inverse Galois Problem: there exist finite groups G which do not have a realization $F/\mathbb{Q}(T)$ that induces all Galois extensions $L/\mathbb{Q}(U)$ of group G by specializing T to $f(U) \in \mathbb{Q}(U)$. For these groups, we produce two extensions $L/\mathbb{Q}(U)$ that cannot be simultaneously induced, thus even disproving a weaker Lifting Property. Our examples of such groups G include symmetric groups S_n , $n \geq 7$, infinitely many $\mathrm{PSL}_2(\mathbb{F}_p)$, the Monster. Two variants of the question with $\mathbb{Q}(U)$ replaced by $\mathbb{C}(U)$ and \mathbb{Q} are answered similarly, the second one under a diophantine “working hypothesis” going back to a problem of Schinzel. We introduce two new tools: a comparizon theorem between the invariants of an extension $F/\mathbb{C}(T)$ and those obtained by specializing T to $f(U) \in \mathbb{C}(U)$; and, given two regular Galois extensions of $k(T)$, a finite set of polynomials $P(U, T, Y)$ that say whether these extensions have a common specialization E/k .

1. INTRODUCTION

Given two fields $k \subset K$, a finite Galois extension $F/k(T)$ and a point $t_0 \in \mathbb{P}^1(K)$, there is a well-defined notion of *specialized extension* F_{t_0}/K (see *Basic terminology*). If F is the splitting field over $k(T)$ of a polynomial $P \in k[T, Y]$, monic in Y , irreducible in $\bar{k}[T, Y]$ and t_0 not a root of the discriminant $\Delta_P \in k[T]$ of P w.r.t Y , F_{t_0} is the splitting field over K of the polynomial $P(t_0, Y)$. We are mostly interested in the situations $K = k$ and $K = k(U)$ (with U a new indeterminate).

The specialization process has been much studied towards the *Hilbert irreducibility* issue of existence of specializations $t_0 \in k$ preserving the Galois group. Investigating the set, say $\mathcal{Sp}_K(F/k(T))$, of all specialized extensions F_{t_0}/K with $t_0 \in \mathbb{P}^1(K)$ is a further goal. For $k = K = \mathbb{Q}$,

Date: May 31, 2016.

2010 Mathematics Subject Classification. Primary 12F12, 11R58, 14E20, ; Secondary 14E22, 12E30, 11Gxx.

Key words and phrases. Galois extensions, inverse Galois theory, specialization, parametric extensions, twisting.

Acknowledgment. This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01).

[Dèbar] shows for example that the number of extensions F_{t_0}/\mathbb{Q} of group $G = \text{Gal}(F/\mathbb{Q}(T))$ and discriminant $|d_E| \leq y$ grows at least like a power of y , for some positive exponent, thereby proving for G the “lower bound part” of a conjecture of Malle.

Little was known on an even more fundamental question: whether $\mathcal{S}p_K(F/k(T))$ can contain all Galois extensions E/K of group contained in $G = \text{Gal}(F/k(T))$; we then say that $F/k(T)$ is *K-parametric*, as for example $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$. Strikingly no group was known yet *not to have* a \mathbb{Q} -parametric or a $\mathbb{Q}(U)$ -parametric extension $F/\mathbb{Q}(T)$ while only four: $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3 , are known to have one. No group with no $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ was even known, while only a few more with one are: cyclic groups, dihedral groups D_{2n} with n odd.

1.1. Groups with no K-parametric extension $F/k(T)$. We produce many such groups:

- a) $k = \mathbb{C}$ and $K = \mathbb{C}(U)$: *non cyclic nilpotent groups G of odd order, symmetric groups S_n with $n \geq 5$, alternating groups A_n with $n \geq 6$, linear groups $\text{PSL}_2(\mathbb{F}_p)$ with $p > 7$ prime, all sporadic groups, etc.*
- b) $k = \mathbb{Q}$ and $K = \mathbb{Q}(U)$: *the same S_n and A_n except for $n = 6$, the $\text{PSL}_2(\mathbb{F}_p)$ with $\binom{2}{p} = \binom{3}{p} = -1$, the Monster M , etc.*
- c) $k = K = \mathbb{Q}$: *the same last groups, under some “working hypothesis”.*

We say more about the “working hypothesis” in §1.4 below and full statements are in §2.3-2.4.

These results fit in the framework of Inverse Galois Theory, a prominent open problem of which is the *Regular Inverse Galois Problem*: is every finite group the Galois group of some extension $F/\mathbb{Q}(T)$ that is \mathbb{Q} -regular, *i.e.* $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$? Possessing a $\mathbb{Q}(U)$ -parametric extension $F/\mathbb{Q}(T)$ is for a group G a strong variant. Our results show that this strong variant fails and that conditionally so does the weaker \mathbb{Q} -parametric analog, thereby setting boundaries for inverse Galois theory over \mathbb{Q} , a topic where few general statements were available. Narrowing these boundaries further, *e.g.* removing “conditionally” in the version over \mathbb{Q} , still remains desirable. We note this weaker but unconditional result¹ of Legrand [Leg16a]: every non trivial group that has at least one \mathbb{Q} -regular realization $F/\mathbb{Q}(T)$ has one that is not \mathbb{Q} -parametric.

1.3. The Lifting Property. Our best result is in fact stronger than the non-existence of parametric extensions and may also be more informative, in that it shows better the obstruction to having a parametric

¹Remark 2.14 explains how Legrand’s result can be deduced from ours under our working hypothesis.

extension that our method reveals, which is not the absence of regular realizations $F/k(T)$ but the existence of several that cannot be “simultaneously lifted”. Specifically, for every group G in list a) above with $k = \mathbb{C}$, or, in list b) with $k \subset \mathbb{C}$, excluding $G = A_n^2$, we show that

(*) *there exist two k -regular Galois extensions $L_1/k(U)$ and $L_2/k(U)$ of group G with this property: there is no k -regular Galois extension $F/k(T)$ of group G such that $F\mathbb{C}/\mathbb{C}(T)$ specializes to $L_1\mathbb{C}/\mathbb{C}(U)$ and $L_2\mathbb{C}/\mathbb{C}(U)$ at two points $T_{01}, T_{02} \in \mathbb{C}(U)$.*

In geometrical terms, this shows that the following *Lifting Property* ($\text{LP}_k(G)$) *any N k - G -Galois covers of \mathbb{P}_k^1 of group G can be, after scalar extension to \mathbb{C} , obtained by pull-back along a map $\mathbb{P}_{\mathbb{C}}^1 \rightarrow \mathbb{P}_{\mathbb{C}}^1$ from some k - G -Galois cover $f : X \rightarrow \mathbb{P}_k^1$ of group G .*

fails for $N = 2$. Thus in the chain of implications (for each $N \geq 2$):

$$\begin{array}{ccccc} G \text{ has a} & & & & G \text{ is a regular} \\ k(U)\text{-parametric} & \Rightarrow & \text{LP}_k(G) & \Rightarrow & \text{Galois group} \\ \text{extension } F/k(T) & & \text{holds for } N & & \text{over } k \end{array}$$

not only the first condition fails, but also the second one.

Our Lifting Property further relates to some variant investigated by Colliot-Thélène [CT00], about which he also obtains a negative conclusion, for some p -group G over some “large” field and he observes that “other examples remain to be seen”.

1.4. parametric vs. generic. As a consequence of our results, the groups from list §1.1 a) do not have a *generic* extension $F/\mathbb{C}(T)$; indeed *generic* is a stronger notion meaning “ L -parametric for all fields $L \supset \mathbb{C}$ ”. This was already known by a result of Buhler-Reichstein [BR97]: the only groups to have a generic extension $F/\mathbb{C}(T)$ are the cyclic groups and dihedral groups D_{2n} with n odd. Our non $\mathbb{C}(U)$ -parametric conclusion however is stronger: the extensions to be parametrized in the generic context include all Galois extensions E/L of group G with L *any field containing \mathbb{C}* and it readily follows that G should then be a subgroup of $\text{PGL}_2(\mathbb{C})$ [JLY02, prop.8.14]. This is an important preliminary reduction for generic extensions that can no longer be used if $F/\mathbb{C}(T)$ is only $\mathbb{C}(U)$ -parametric (*i.e.* only parametrizes extensions $E/\mathbb{C}(U)$). There exist in fact groups that have a $\mathbb{C}(U)$ -parametric extension but no generic extension $F/\mathbb{C}(T)$ (corollary 2.4).

²For $G = A_n$, the two extensions $L_i/k(U)$ from (*) should be replaced by three.

1.5. The comparizon theorem. We will first focus on the situation $K = k(U)$ with $k \subset \mathbb{C}$. Results mentioned above follow from a general criterion (criterion 2.6) for some set of k -regular Galois extensions $L/k(U)$ of group G to be $k(U)$ -specializations of a k -regular Galois extension $F/k(T)$ of group G . A main point of our approach is that

(*) *the branch point number of an extension³ $F/\mathbb{C}(T)$ cannot drop under specialization of T in $\mathbb{C}(U)$, unless $F/\mathbb{C}(T)$ is one from a list of exceptional extensions with F of genus 0 (see theorem 2.1 (a)).*

Despite its basic nature, this did not seem to be known; the difficulty is that the group may drop and that the ramification of the specialization point $T_0 \in \mathbb{C}(U)$ may cancel some of the ramification of $F/\mathbb{C}(T)$. We prove a more precise version giving better estimates of the branch point number and other invariants of specialized extensions $F_{T_0}/\mathbb{C}(U)$, $T_0 \in \mathbb{C}(U)$, which could be interesting beyond this paper (theorem 3.1).

1.6. A pre-order on Galois extensions $L/\mathbb{C}(T)$. The situation $K = \mathbb{C}(U)$ has another interesting feature: specialized extensions $F_{T_0}/\mathbb{C}(U)$ with $T_0 \in \mathbb{C}(U)$ remain extensions of the rational function field in one indeterminate, as the initial extension $F/\mathbb{C}(T)$. The specialization process induces a (partial) pre-order on the set of Galois extensions $L/\mathbb{C}(T)$. We will show that this is in fact an order on a big subset (see theorem 2.1 (b)), with this consequence:

(*) *for “most” groups G (e.g. all groups of rank ≥ 4), there is at most one $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ of group G .*

The pre-order that we use to investigate the minimal elements raises further questions about the ordered structure of Galois extensions of $k(T)$ that are certainly worthwhile being studied.

1.7. The twisted polynomial. Our results in the situation that $k = K$ is a number field will be obtained from those with $K = k(U)$ by specialization, but of the indeterminate U this time. To this end we will generalize a tool introduced in [Dèbar] as the “self-twisted cover”. Theorem 2.11 is the concrete statement that makes this specialization approach work. It is interesting for its own sake: given two k -regular Galois extensions $F/k(T)$, $L/k(T)$ of group G , it provides a finite set of polynomials $\tilde{P}_F^L(U, T, Y) \in k[U, T, Y]$ which have the answer to the question of whether $F/k(T)$ and $L/k(T)$ have a common specialization:

(*) *for all but finitely many $u_0 \in k$, $L_{u_0}/k = F_{t_0}/k$ for some $t_0 \in k$ not a branch point of $F/k(T)$ if and only if one of the polynomials*

³The extension $F/\mathbb{C}(T)$ need not be assumed to be Galois in this statement.

$\tilde{P}_F^L(u_0, t_0, Y)$ has a root $y_0 \in k$; and similarly, $L_U/k(U) = F_{T_0}/k(U)$ for some $T_0 \in k(U)$ iff one polynomial $\tilde{P}_F^L(U, T_0, Y)$ has a root $Y_0 \in k(U)$.

The working hypothesis, which goes back to some diophantine problem of Schinzel, relates the absence of $k(U)$ -rational points $(T_0, Y_0) \in k(U)^2$ on each of the curves $\tilde{P}_F^L(U, T, Y) = 0$ to the absence, for infinitely many $u_0 \in k$, of k -rational points $(t_0, y_0) \in k^2$ on each of the curves $\tilde{P}_F^L(u_0, T, Y) = 0$ (see §2.4.2), thereby extending Hilbert's Irreducibility Theorem to polynomials with two indeterminates and one parameter. It has no known counter-example.

The paper is organized as follows. §2 presents in full detail the results of our paper. We reduce their proofs to that of two main theorems: the comparizon theorem 2.1 and the “twisting” theorem 2.11. We state them and explain their implications. Their proofs, which are rather independent, are given in §3 and §4. Finally §5 is an appendix where we have collected a few classical results that enter in our proofs and that we have rephrased to fit our field arithmetic set-up; this section is used in §3 and in §4. We start below with some basic terminology.

BASIC TERMINOLOGY (for more details, see [DD97] or [DL13]).

The base field k is always assumed to be of characteristic 0. Is also fixed a big algebraically closed field containing the complex field \mathbb{C} and the indeterminates that will be used and in which all field compositum should be understood.

Given a field K , an extension $F/K(T)$ is said to be ***K-regular*** if $F \cap \overline{K} = K$. We make no distinction between a K -regular extension $F/K(T)$ and the associated K -regular cover $f : X \rightarrow \mathbb{P}^1$: f is the normalization of \mathbb{P}_K^1 in F and F is the function field $K(X)$ of X . The “field extension” viewpoint is mostly used in this paper.

We also use ***affine equations***: we mean the irreducible polynomial $P \in K[T, Y]$ of a primitive element of $F/K(T)$, integral over $K[T]$.

By ***group*** and ***branch point set*** of a K -regular extension $F/K(T)$, we mean those of the extension $F\overline{K}/\overline{K}(T)$: the group of $F\overline{K}/\overline{K}(T)$ is the Galois group of its Galois closure. The branch point set of $F\overline{K}/\overline{K}(T)$ is the (finite) set of points $t \in \mathbb{P}^1(\overline{K})$ such that the associated discrete valuations are ramified in $F/\overline{K}(T)$.

The field K being of characteristic 0, we also use the ***inertia canonical invariant***⁴ \mathbf{C} of the K -regular extension $F/K(T)$, defined as follows. If $\mathbf{t} = \{t_1, \dots, t_r\}$ is the branch point set of f , then \mathbf{C} is a r -tuple (C_1, \dots, C_r) of conjugacy classes of the group G of f : for $i = 1, \dots, r$,

⁴This is also called “branching type” by some authors.

C_i is the conjugacy class of the distinguished⁵ generators of the inertia groups $I_{\mathfrak{p}}$ above t_i in the Galois closure $\widehat{F}/K(T)$ of $F/K(T)$.

We also use the notation $\mathbf{e} = (e_1, \dots, e_r)$ for the r -tuple with i th entry the ramification index $e_i = |I_{\mathfrak{p}}|$ of primes above t_i ; e_i is also the order of elements of C_i , $i = 1, \dots, r$.

We say that two K -regular extensions $F/K(T)$ and $L/K(T)$ are **isomorphic** if there is a field isomorphism $F \rightarrow L$ that restricts to an automorphism $\chi : K(T) \rightarrow K(T)$ equal to the identity on K and that they are **$K(T)$ -isomorphic** if in addition χ is the identity on $K(T)$.

Given a Galois extension $F/K(T)$ and $t_0 \in \mathbb{P}^1(K)$, the **specialization of $F/K(T)$ at t_0** is the Galois extension F_{t_0}/K defined as follows. Consider the localized ring $A_{t_0} = K[T]_{\langle T-t_0 \rangle}$ of $K[T]$ at t_0 , the integral closure B_{t_0} of A_{t_0} in F . Then F_{t_0}/K the residue extension of an arbitrary prime ideal of B_{t_0} above $\langle T - t_0 \rangle$. (As usual use the local ring $K[1/T]_{\langle 1/T \rangle}$ and its ideal $\langle 1/T \rangle$ if $t_0 = \infty$).

If $P \in K[T, Y]$ is an affine equation of $F/K(T)$ and $\Delta_P \in K[T]$ is its discriminant w.r.t. Y , then for every $t_0 \in K$ such that $\Delta_P(t_0) \neq 0$, t_0 is not a branch point of $F/K(T)$ and the specialized extension F_{t_0}/K is the splitting field over K of $P(t_0, Y)$.

If K' is a field containing K , the **specialization F_{t_0}/K' of $F/K(T)$ at t_0** is the extension $(FK')_{t_0}/K'$. If $K' = K(U)$, $T_0 \in K(U)$ is a non-constant rational function⁶ and $P \in K[T, Y]$ is an affine equation of $F/K(T)$, then $\Delta_P(T_0) \neq 0$ and so $P(T_0(U), Y)$ is an affine equation of the specialized extension $F_{T_0}/K(U)$.

If the extension $F/K(T)$ is not Galois, the above definition leads to several specializations F_{t_0}/K : the prime ideals of B_{t_0} above $\langle T - t_0 \rangle$ are not conjugate in general. When we use this extended definition (only once in theorem 3.1 (a)), we will talk about *a* specialization instead of *the* specialization F_{t_0}/K .

We finally recall the **Riemann Existence Theorem** (RET) which indicates that Galois extensions $F/k(T)$ are well-understood if k is algebraically closed and which we will use in this practical form.

Riemann Existence Theorem. *Given a group G , an integer $r \geq 2$, a subset $\mathbf{t} \subset \mathbb{P}^1(\mathbb{C})$ of r points and an r -tuple $\mathbf{C} = (C_1, \dots, C_r)$ of conjugacy classes of G , there is a Galois extension $F/\mathbb{C}(T)$ of group G , branch point set \mathbf{t} and inertia canonical invariant \mathbf{C} iff there exists*

⁵“distinguished” means that these generators correspond to the e_i th root $e^{2i\pi/e_i}$ of 1 in the canonical isomorphism $I_{\mathfrak{p}} \rightarrow \mu_{e_i} = \langle e^{2i\pi/e_i} \rangle$.

⁶We use a capital letter for the specialization point T_0 to stress that it is a function $T_0(U)$ contrary to the situation for which it is a point in the ground field and the notation t_0 is preferred.

$(g_1, \dots, g_r) \in C_1 \times \dots \times C_r$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \dots, g_r \rangle = G$. Furthermore the number of such extensions $F/\mathbb{C}(T)$ (in a fixed algebraic closure $\overline{k(T)}$) equals the number of r -tuples (g_1, \dots, g_r) as above, counted modulo componentwise conjugation by an element of G .

2. MAIN RESULTS

We present our main results: the specialization process and the associated order in the situation $k = \mathbb{C}$ and $K = \mathbb{C}(U)$ (§2.1), some new examples of groups with a $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ (§2.2), a method to produce groups with no $k(U)$ -parametric extension $F/k(T)$ (§2.3), our “twisted polynomial” $\tilde{P}_F^L(U, T, Y)$ and its use towards the construction of groups with no k -parametric extension $F/k(T)$ (§2.4).

2.1. $\mathbb{C}(U)$ -specializations of Galois extensions $F/\mathbb{C}(T)$. This subsection gives the main definitions and our first main tool (theorem 2.1).

2.1.1. Comparison theorem. Given a K -regular extension $F/K(T)$, we use the following notation for its *invariants*: G_F for the group, r_F for the branch point number, \mathbf{C}_F for the inertia canonical invariant and g_F for the genus of F ; they are invariant inside the isomorphism class of $F/K(T)$.

Given two Galois extensions $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$, we write

$$F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$$

if $L/\mathbb{C}(U)$ is the specialization $F_{T_0}/\mathbb{C}(U)$ of $F/\mathbb{C}(T)$ at some non-constant rational function $T_0 \in \mathbb{C}(U)$.

For a conjugacy class C of a group G , set $C^{\mathbb{Z}} = \bigcup_{\alpha \in \mathbb{Z}} C^\alpha$; $C^{\mathbb{Z}}$ corresponds to the conjugacy class of the cyclic subgroup generated by any element of C . Given tuples $\mathbf{C} = (C_1, \dots, C_r)$ and $\mathbf{C}' = (C'_1, \dots, C'_r)$ of conjugacy classes of G and G' , write $\mathbf{C} \prec \mathbf{C}'$ if for every $j \in \{1, \dots, r\}$, there exists $i \in \{1, \dots, r\}$ such that $C'_j \subset C_i^{\mathbb{Z}}$.

Theorem 2.1. (a) *Let $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$ be two finite Galois extensions. Assume $g_F \geq 1$. Then we have:*

$$F/\mathbb{C}(T) \prec L/\mathbb{C}(T) \Rightarrow (G_F, r_F, \mathbf{C}_F) \prec (G_L, r_L, \mathbf{C}_L)$$

where the right-hand side condition means that $G_F \supset G_L$, $r_F \leq r_L$ and $\mathbf{C}_F \prec \mathbf{C}_L$. If in addition $G_F = G_L$, the implication also holds if $g_F = 0$; and we have $g_F \leq g_L$ if $r_F \geq 4$.

As recalled in §3.3, the excluded case $g_F = 0$ is known to only happen when $r_F \leq 3$ and G_F is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$, i.e., one of these groups: $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 1$), $(\mathbb{Z}/2\mathbb{Z})^2$, A_4 , S_4 , A_5 , D_{2n} ($n \geq 3$). For each

such group G_F , there is, up to isomorphism, only one Galois extension $F/\mathbb{C}(T)$ of group G_F and genus $g_F = 0$.

Theorem 2.1 will be deduced from theorem 3.1 which offers more precise estimates, for example, the lower bound

$$(*) \quad r_L \geq (N - 4)r_F + 4$$

if $L/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$ with $T_0 \in \mathbb{C}(T)$ of degree N .

2.1.2. *The order \prec .* These estimates will further show that, as stated below, the pre-order \prec is antisymmetric on a big subset of all Galois extensions, regarded modulo isomorphisms.

Specifically, denote by \mathcal{G}^* the set of groups that are

(*) (of rank ≥ 4) or (or rank 3 and odd order) or (of rank 2 and order not divisible by 2 or 3) or (a subgroup of $\mathrm{PGL}_2(\mathbb{C})$)

and by \mathcal{E}^* the set of all Galois extensions $F/\mathbb{C}(T)$, viewed up to isomorphism such that $(G_F \in \mathcal{G}^*, G_F \not\subset \mathrm{PGL}_2(\mathbb{C}))$ or $(g_F = 0)$.

The notion of “parametric extensions” appearing below was introduced in §1; the definition is recalled right next in §2.1.3.

Theorem 2.1. (b) *The relation \prec induces a (partial) order on \mathcal{E}^* . Consequently, for every group $G \in \mathcal{G}^*$, there is at most one Galois extension $F/\mathbb{C}(T)$ of group G that is $\mathbb{C}(U)$ -parametric.*

The uniqueness part follows from the first part: the main point is that if an extension $F/\mathbb{C}(T)$ is $\mathbb{C}(U)$ -parametric of group $G \in \mathcal{G}^*$, it is the smallest (for \prec) Galois extension $L/\mathbb{C}(T)$ of group G .⁷

We have no example of two non-isomorphic Galois extensions $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$ such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$ and $L/\mathbb{C}(T) \prec F/\mathbb{C}(T)$, and in particular, no example of a group G that has two $\mathbb{C}(U)$ -parametric extensions $F/\mathbb{C}(T)$. In fact the groups that are known to have at least one $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ are the finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$, and for them, uniqueness is part of theorem 2.1 (for the existence, see corollary 2.4).

The proofs of the two parts of theorem 2.1 are given in §3.2 and §3.4.

2.1.3. *Parametric extensions.* The following definition was introduced by F. Legrand [Leg13], [Legar], [Leg15]. Close variants exist in connection with the notion of generic polynomials [JLY02].

Definition 2.2. A finite k -regular Galois extension $F/k(T)$ of group G is *k -parametric* if for every Galois extension E/k of group contained in

⁷For a Galois extension $L/\mathbb{C}(T)$ of group G , there is a Galois extension $F/\mathbb{C}(T)$ such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$ and $F/\mathbb{C}(T)$ is minimal (for \prec) among all Galois extensions of $\mathbb{C}(T)$ of group G . Several such extensions $F/\mathbb{C}(T)$ exist in general.

G , there exists $t_0 \in \mathbb{P}^1(k)$, not a branch point of $F/k(T)$, such that the specialized extension F_{t_0}/k is k -isomorphic to E/k . Given an overfield $K \supset k$, $F/k(T)$ is K -parametric if $FK/K(T)$ is K -parametric. The group G is then said to have a K -parametric extension $F/k(T)$.

The extension $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ is the standard example of an extension $F/\mathbb{Q}(T)$ that is K -parametric; it is for all fields $K \supset \mathbb{Q}$ and so is in fact generic. Recall indeed that “generic” for a finite k -regular Galois extension $F/k(T)$ means “ K -parametric for all fields $K \supset k$ ”.

Remark 2.3. (a) A $k(U)$ -parametric extension $F/k(T)$ is k -parametric.

Proof. Let $F/k(T)$ be a $k(U)$ -parametric extension of group G . The extension $Fk(U)/k(U, T)$ is $k(U)$ -regular and *a fortiori* the extension $F/k(T)$ is k -regular. Let E/k be a Galois extension of group $H \subset G$. As $F/k(T)$ is $k(U)$ -parametric, there is $T_0 \in k(U)$ such that the specialized extension $F_{T_0}/k(U)$ is $k(U)$ -isomorphic to $E(U)/k(U)$. Hence for all but finitely many $u_0 \in \mathbb{P}^1(k)$, the extension, $(F_{T_0})_{u_0}/k$, obtained by specializing $F_{T_0}/k(U)$ at u_0 is E/k . The conclusion follows since, as explained below, for all but finitely many $u_0 \in \mathbb{P}^1(k)$, $(F_{T_0})_{u_0}/k$ is also the specialized extension $F_{T_0(u_0)}/k$.

This is clear if $T_0 \in k$. Assume $T_0 \notin k$ and let $P \in k[T, Y]$ be an affine equation of $F/k(T)$. Then F_{T_0} is the splitting field over $k(U)$ of $P(T_0(U), Y)$ and, as $F/k(T)$ is Galois, it is also the splitting field of any irreducible factor $Q \in k[U, Y]$ of $P(T_0(U), Y)$. Thus such a Q is an affine equation of the Galois extension $F_{T_0}/k(U)$. For all but finitely many $u_0 \in \mathbb{P}^1(k)$, the extension $(F_{T_0})_{u_0}/k$ is the splitting field over k of $Q(u_0, Y)$ and also of $P(T_0(u_0), Y)$. This concludes the argument as for all but finitely many $u_0 \in \mathbb{P}^1(k)$, $F_{T_0(u_0)}/k$ is also the splitting field over k of $P(T_0(u_0), Y)$. \square

This argument applies inductively to show that condition “ $F/k(T)$ is $k(U_1, \dots, U_s)$ -parametric” is stronger and stronger as s gets bigger; it remains however always weaker than “generic”.

(b) On the other hand, for a k -regular Galois extension $F/k(T)$ and an algebraic extension E/K with $K \supset k$, the connection between “ E -parametric” and “ K -parametric” is not so clear. As we will see, our criterion to produce non $k(U)$ -parametric extensions is all the more efficient that there are more $k(U)$ -regular realizations of the group G in question, and so will be more fruitful when k is algebraically closed. We however do not have any proof of any implication.

2.2. Groups with a $k(U)$ -parametric extension $F/k(T)$. We have the following statement.

Corollary 2.4. *All subgroups of $\mathrm{PGL}_2(\mathbb{C})$:*

$$\mathbb{Z}/n\mathbb{Z} \ (n \geq 1), \ (\mathbb{Z}/2\mathbb{Z})^2, \ A_4, \ S_4, \ A_5, \ D_{2n} \ (n \geq 3)$$

have a $\mathbb{C}(U)$ -parametric extension. Out of them, $\mathbb{Z}/n\mathbb{Z}$ with $n = 1, 2, 3$ and $D_6 = S_3$ have a $k(U)$ -parametric extension for every field k of characteristic 0.

Theorem 2.1 (b) shows further that the $\mathbb{C}(U)$ -parametric extension claimed to exist is unique up to isomorphism.

Proof. The first part is a consequence of corollary 4.2; the main points are the “twisting lemma” and Tsen’s theorem. The four groups in the second part are known to have a generic extension $F/\mathbb{Q}(T)$ [JLY02] \square

Remark 2.5 (Parametricity and genericity). Cyclic groups and dihedral groups D_{2n} with n odd were known to have a $\mathbb{C}(U)$ -parametric extension as they have a generic extension $F/\mathbb{C}(T)$: for $\mathbb{Z}/d\mathbb{Z}$, take $F = \mathbb{C}(T^{1/d})/\mathbb{C}(T)$ ($d \geq 1$); for D_{2n} , it is a result of Hashimoto-Miyake [HM99] (see also [JLY02, theorem 5.5.4]). These groups are the only ones to have a generic extension $F/\mathbb{C}(T)$ [BR97]. The other subgroups of $\mathrm{PGL}_2(\mathbb{C})$: $(\mathbb{Z}/2\mathbb{Z})^2, A_4, S_4, A_5, D_{2n}$ with n even, have a $\mathbb{C}(U)$ -parametric extension but no generic extension $F/\mathbb{C}(T)$. Whether subgroups of $\mathrm{PGL}_2(\mathbb{C})$ other than $\mathbb{Z}/n\mathbb{Z}$ with $n = 1, 2, 3$ and S_3 have a $\mathbb{Q}(U)$ -parametric extension $F/\mathbb{Q}(T)$ is unclear.⁸

2.3. Groups with no $k(U)$ -parametric extension $F/k(T)$. We explain how we use theorem 2.1 to produce groups with no $k(U)$ -parametric extension $F/k(T)$, with k algebraically closed in §2.3.2 and k non algebraically closed in §2.3.3. We start with a general criterion in §2.3.1. For simplicity, assume $k \subset \mathbb{C}$; there is no loss of generality.

Our method will in fact lead to a slightly better conclusion than “no $k(U)$ -parametric extension”. To this end we define a k -regular Galois extension $F/k(T)$ to be *weakly $k(U)$ -parametric* of group G if for every k -regular Galois extension $L/k(U)$ of group G (and not of group *contained in* G as for $k(U)$ -parametric), $L\mathbb{C}/\mathbb{C}(U)$ is a specialization $F_{T_0}/\mathbb{C}(U)$ for some $T_0 \in \mathbb{C}(U)$ (while for $k(U)$ -parametric, the requested T_0 is in $k(U)$). Obviously we have:

$$k(U)\text{-parametric} \Rightarrow \text{weakly } k(U)\text{-parametric}$$

⁸Even if for some of these groups ($(\mathbb{Z}/2\mathbb{Z})^2, S_4, D_{2n}$ with n even), the unique $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ is defined over \mathbb{Q} (§3.3), a \mathbb{Q} -model $F_0/\mathbb{Q}(T)$ is not guaranteed to be $\mathbb{Q}(U)$ -parametric: although any extension $L/\mathbb{Q}(U)$ of group G is a specialization of $F/\mathbb{C}(T)$, the specialization point T_0 , which is in $\mathbb{C}(U)$ may not be in $\mathbb{Q}(U)$. Anticipating on §4.2, the issue relates to the following: a polynomial equation $P(U, T, Y) = 0$ with $P \in \mathbb{Q}[U, T, Y]$ may have a solution $(T_0(U), Y_0(U)) \in \mathbb{C}(U)^2$ but no solution in $\mathbb{Q}(U)^2$: think of $Y^2 + T^2 + U^2 + 1 = 0$.

2.3.1. *General criterion.* Given a subfield $k \subset \mathbb{C}$ and a finite group G , denote the set of all k -regular extensions $L/k(T)$ of group G by $\mathcal{R}_k(G)$. From theorem 2.1, if $F/k(T)$ is a weakly $k(U)$ -parametric extension of group G , we must have $(G, r_F, \mathbf{C}_F) \prec (G, r_L, \mathbf{C}_L)$ for every extension $L/k(T) \in \mathcal{R}_k(G)$. The general idea is to show that there is no Galois extension $F/\mathbb{C}(T)$ of group G such that

$$(*) \quad r_F \leq r_L \text{ and } \mathbf{C}_F \prec \mathbf{C}_L \text{ for every } L/k(T) \in \mathcal{R}_k(G).$$

Criterion 2.6 below uses the following additional notation. Say that two conjugacy classes C and C' of G are *very different*, and write then $C \# C'$ if there is no conjugacy class C_0 such $C \subset C_0^{\mathbb{Z}}$ and $C' \subset C_0^{\mathbb{Z}}$. For example, if C is the conjugacy class of a generator of a maximal cyclic subgroup of G , then $C \# C'$ if and only if $C' \not\subset C^{\mathbb{Z}}$. In particular, if C' is also the conjugacy class of a generator of a maximal cyclic subgroup of G , then $C \# C'$ if and only if $C^{\mathbb{Z}} \neq (C')^{\mathbb{Z}}$, i.e., if the two maximal cyclic subgroups associated with C and C' are not conjugate in G . Many concrete examples appear in §2.3.2 and §2.3.3 below.

Criterion 2.6. *Let \mathcal{R} be a nonempty subset of $\mathcal{R}_k(G)$. Let $\rho_{\mathcal{R}}$ be the minimum number r_L for some $L/k(T) \in \mathcal{R}$. Assume the list of conjugacy classes C appearing in some tuple \mathbf{C}_L with $L/k(T) \in \mathcal{R}$ contains at least $\nu_{\mathcal{R}}$ of them that are pairwise very different, and that $\nu_{\mathcal{R}} > \rho_{\mathcal{R}}$. (***) Then there is no k -regular Galois extension $F/k(T)$ of group G that admits each extension $L\mathbb{C}/\mathbb{C}(U) \in \mathcal{R}$ as a specialization $F_{T_0}/\mathbb{C}(U)$ for some $T_0 \in \mathbb{C}(U)$ (depending on $L\mathbb{C}/\mathbb{C}(U)$).*

In particular, G has no weakly $k(U)$ -parametric extension and a fortiori no $k(U)$ -parametric extension $F/k(T)$.

The smaller the subset \mathcal{R} is the stronger is conclusion (**), which, in the extreme case $\mathcal{R} = \mathcal{R}_k(G)$, is equivalent to G not having a weakly $k(U)$ -parametric extension $F/k(T)$.

Proof. Assume that there is a k -regular Galois extension $F/k(T)$ of group G such that $F\mathbb{C}/\mathbb{C}(T)$ specializes to each of the extensions $L\mathbb{C}/\mathbb{C}(T)$ with $L/k(T) \in \mathcal{R}$. It follows from theorem 2.1 that $r_F \leq \rho_{\mathcal{R}}$ and $\mathbf{C}_F \prec \mathbf{C}_L$ for every $L/k(T) \in \mathcal{R}$. Hence if C, C' are two conjugacy classes appearing in the list of tuples \mathbf{C}_L with $L/k(T) \in \mathcal{R}$, there are conjugacy classes $C_{F,i}, C_{F,j}$ from \mathbf{C}_F such that $C \subset C_{F,i}^{\mathbb{Z}}$ and $C' \subset C_{F,j}^{\mathbb{Z}}$. If $C \# C'$, then $C_{F,i} \neq C_{F,j}$. Therefore $r_F \geq \nu_{\mathcal{R}}$. Hence $\rho_{\mathcal{R}} \geq \nu_{\mathcal{R}}$, a contradiction. \square

2.3.2. *Groups with no $\mathbb{C}(U)$ -parametric extension.* Denote the number of conjugacy classes of maximal cyclic subgroups of a group G by $\nu(G)$ and the rank of G (minimal cardinality of a generating set) by $\text{rk}(G)$.

Corollary 2.7. *Assume k is algebraically closed. If $\nu(G) \geq \text{rk}(G) + 2$, conclusion (**) from criterion 2.6 holds with \mathcal{R} consisting of two extensions $L_1/k(T)$ and $L_2/k(T)$. Consequently G has no weakly $k(U)$ -parametric extension and a fortiori no $k(U)$ -parametric extension $F/k(T)$.*

Proof. This directly follows from criterion 2.6 applied with \mathcal{R} consisting of two extensions $L_1/k(T)$ and $L_2/k(T)$ chosen so that $r_{L_1} = \text{rk}(G) + 1$ and \mathbf{C}_{L_2} contains all non trivial conjugacy classes of G . Such extensions exist thanks to the RET. \square

As we check below, the groups in the following non exhaustive list satisfy the condition $\nu(G) \geq \text{rk}(G) + 2$.

Corollary 2.8. *Assume k is algebraically closed. None of these groups:*

- S_n , $n \geq 5$ and A_n , $n \geq 6$,
- non cyclic nilpotent groups G with abelianization G^{ab} different from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, in particular non cyclic nilpotent groups G of odd order,
- linear groups $\text{PSL}_2(\mathbb{F}_p)$, $p > 7$ prime,
- all sporadic simple groups,

*have a weakly $k(U)$ -parametric extension $F/k(T)$. More precisely conclusion (**) from criterion 2.6 holds with $k = \mathbb{C}$ and \mathcal{R} consisting of two extensions except for the groups A_n for which three are needed.*

On the other hand, all finite subgroups of $\text{PGL}_2(\mathbb{C})$ can be double-checked not to satisfy $\nu(G) \geq \text{rk}(G) + 2$ (which must also hold because they have a $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$). The quaternion group \mathbb{H}_8 is another example. The complete list of groups satisfying the condition remains to be established. It seems that it contains most simple groups (and not just the last two categories of examples).

Proof. We use the standard notation for the conjugacy classes of S_n : $[1^{\ell_1} \dots n^{\ell_n}]$ is the conjugacy class of elements of S_n that write as a product of ℓ_1 cycles of length 1, ..., ℓ_n cycles of length n , all cycles having disjoint supports.

The symmetric groups S_n , $n \geq 5$, satisfy $\nu(G) \geq \text{rk}(G) + 2$. Indeed $\text{rank}(S_n) = 2$ and the 4 conjugacy classes

$$[n^1], [(n-1)^1], [(n-2)^1 2^1], [2^1]$$

are pairwise very different.

So do the alternating groups A_n with $n \geq 6$: note that $\text{rank}(A_n) = 2$ and use the classes

$$\begin{cases} [n^1], [(n-3)^1 2^1], [(n-2)^1 1^2], [(n-4)^1 1^4] & \text{if } n \text{ odd} \\ [(n-1)^1], [(n-2)^1 2^1], [(n-3)^3 1], [(n-5)^1 1^5] & \text{if } n \text{ even} \end{cases}$$

For the second class of examples, we start with the case G is abelian. If G of rank $s \geq 2$, it then writes $G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_s\mathbb{Z}$ with $s \geq 2$ and $d_1|d_2|\cdots|d_s$ in \mathbb{Z} . The s -tuples $(\varepsilon_1, \dots, \varepsilon_{s-1}, 1)$ with $\varepsilon_i \in \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_{s-1}\mathbb{Z}$ generate non-conjugate maximal cyclic subgroups of G . There are $d_1 \cdots d_{s-1}$ such s -tuples, and so at least $s + 2$ unless $(s = 2$ and $d_1 \in \{2, 3\})$ or $(s = 3$ and $d_1 = d_2 = 2)$. After checking separately the remaining special cases (use further non-conjugate maximal cyclic subgroups *e.g.* those generated by s -tuples $(\varepsilon_1, \dots, \varepsilon_{s-1}, k)$ with $k \in (\mathbb{Z}/d_s\mathbb{Z})^\times$), conclude that $\nu(G) \geq \text{rk}(G) + 2$ unless $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Assume now more generally that G is nilpotent. From the Burnside basis theorem, G and its abelianization G^{ab} have the same rank. On the other hand, we have $\nu(G) \geq \nu(G^{\text{ab}})$. If G is non cyclic then so is G^{ab} . If G^{ab} is further assumed to be different from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then from the preceding case, we have $\nu(G^{\text{ab}}) \geq \text{rk}(G^{\text{ab}}) + 2$. Inequality $\nu(G) \geq \text{rk}(G) + 2$ follows.

All finite simple groups have rank 2 and their well-known classification shows that many of them have at least 4 non-conjugate maximal cyclic subgroups of G , including all groups $\text{PSL}_2(\mathbb{F}_p)$ ($p > 7$ prime), all sporadic simple groups. \square

Remark 2.9. Depending on the problem and the situation, the general method can be used differently and leads to variants of corollary 2.7. Here is an example:

(*) *If N is the largest integer $< \nu(G)/(\text{rk}(G) + 1)$, there do not exist N Galois extensions $F_1/\mathbb{C}(T), \dots, F_N/\mathbb{C}(T)$ of group G such that every extension $L/\mathbb{C}(U)$ of group G is a specialization $(F_i)_{T_0}/\mathbb{C}(U)$ of some $F_i/\mathbb{C}(T)$, $i = 1, \dots, N$ (for some $T_0 \in \mathbb{C}(U)$).*

Proof. Let $g_1, \dots, g_{\nu(G)}$ be generators of $\nu(G)$ non-conjugate maximal cyclic subgroups and let $C_1, \dots, C_{\nu(G)}$ be their conjugacy classes. For $i = 1, \dots, \nu(G)$, construct a Galois extension $L_i/\mathbb{C}(T)$ such that C_i appears in \mathbf{C}_{L_i} , $r_{L_i} = \text{rk}(G) + 1$, and in such a way that the constructed extensions are distinct; if two extensions happen to be equal in a first stage, compose one with a non-trivial automorphism of $\mathbb{C}(T)$. Assume that there exist N Galois extensions $F_1/\mathbb{C}(T), \dots, F_N/\mathbb{C}(T)$ satisfying the conclusion of the claim. Then there is an index $i \in \{1, \dots, N\}$ such that $F_i/\mathbb{C}(T)$ specializes to at least $\nu(G)/N$ of the constructed extensions $L/\mathbb{C}(T)$. If \mathcal{R} is the set of these extensions $L/\mathbb{C}(T)$, we have $\rho_{\mathcal{R}} = \text{rk}(G) + 1$ and criterion 2.6 can be applied with $\nu_{\mathcal{R}} \geq \nu(G)/N$; this gives $\nu(G)/N \leq \text{rk}(G) + 1$ and so $N \geq \nu(G)/(\text{rk}(G) + 1)$.

2.3.3. *Groups with no $\mathbb{Q}(U)$ -parametric extension.* Here we apply criterion 2.6 over a non-algebraically closed field k .

Corollary 2.10. *Let k be a subfield of \mathbb{C} . None of the groups*

- S_n , $n \geq 5$ and $n \neq 6$ and A_n , $n \geq 7$,
- $\mathrm{PSL}_2(\mathbb{F}_p)$ with p a prime such that $(\frac{2}{p}) = (\frac{3}{p}) = -1$,
- the Fischer-Griess Monster M ,

*have a weakly $k(U)$ -parametric extension $F/k(T)$ and a fortiori they do not have a $k(U)$ -parametric extension. More precisely conclusion $(**)$ from criterion 2.6 holds with $k = \mathbb{Q}$ and \mathcal{R} consisting of two extensions except the alternating groups A_n for which three are needed.*

The list is not exhaustive. This corollary is meant to show on examples how to apply criterion 2.6 and how in some situations where it cannot be applied directly, one can still get the desired conclusion.

Proof. Take $G = S_n$, $n \geq 5$, $n \neq 6$. Assume first n is odd. There are \mathbb{Q} -regular realizations $L_1/\mathbb{Q}(T)$, $L_2/\mathbb{Q}(T)$ of S_n with $r_{L_1} = r_{L_2} = 3$ and $\mathbf{C}_{L_1} = ([n^1], [(n-1)^1 1^1], [2^1 1^{n-2}])$ & $\mathbf{C}_{L_2} = ([n^1], [(n-2)^1 2^1], [2^1 1^{n-2}])$ (see [Sch00], [Leg13, B-3]). Hence for $\mathcal{R} = \{L_1/\mathbb{Q}(T), L_2/\mathbb{Q}(T)\}$, we have $\rho_{\mathcal{R}} \leq 3$ and one can take $\nu_{\mathcal{R}} \geq 4$ in criterion 2.6. Conclude that $(**)$ is satisfied for this \mathcal{R} . In particular, S_n has no weakly $k(U)$ -parametric extension $F/k(T)$. The case n is even is similar; $L_2/\mathbb{Q}(T)$ should be changed to have $\mathbf{C}_{L_2} = ([n^1], [(n-m)^1 m^1], [2^1 1^{n-2}])$ for some integer m such that $1 \leq m \leq n$ and $(m, n) = 1$.

Take $G = A_n$, $n \geq 7$. The group A_n is known to have \mathbb{Q} -regular realizations with the following inertia canonical invariant [Leg13, B-3]:

if n is even:

$$([m^1(n-m)^1], [m^1(n-m)^1], [(n/2)^2]) \text{ with } 1 \leq m \leq n, (m, n) = 1$$

if n is odd:

$$\begin{aligned} &([n^1], [n^1], [m^1((n-m)/2)^2]) \text{ with } m \text{ odd, } 1 \leq m \leq n, (m, n) = 1, \\ &([n^1], [n^1], [(m/2)^2(n-m)^1]) \text{ with } m \text{ even, } 1 \leq m \leq n, (m, n) = 1 \end{aligned}$$

One checks that for every $n \geq 7$, one can always find three such realizations with four pairwise very different conjugacy classes in the union of the three inertia canonical invariants. Criterion 2.6 concludes that the proof in this case.

Take $G = \mathrm{PSL}_2(\mathbb{F}_p)$ with p a prime such that $(\frac{2}{p}) = -1$ and $(\frac{3}{p}) = -1$. [Ser92, §8.3.3] gives two \mathbb{Q} -regular realizations $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$ of G with $r_{L_1} = r_{L_2} = 3$ and

$$\mathbf{C}_{L_1} = (2A, pA, pB) \text{ \& } \mathbf{C}_{L_2} = (3A, pA, pB)$$

where $2A$ (resp. $3A$) is the unique conjugacy class of $\mathrm{PSL}_2(\mathbb{F}_p)$ of order 2 (resp. of order 3) and pA, pB are the two conjugacy classes of order p . Hence for $\mathcal{R} = \{L_1/\mathbb{Q}(T), L_2/\mathbb{Q}(T)\}$, we have $\rho_{\mathcal{R}} \leq 3$.

According to [GMPS15, corollary 2.7], the maximal order of an element of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $p+1$, so the conjugacy classes pA and pB are classes of generators of maximal cyclic subgroups. It follows that $2A \# pA$, $2A \# pB$, $3A \# pA$, $3A \# pB$. Furthermore $2A \# 3A$: indeed otherwise both classes would be contained in the conjugacy class of a cyclic subgroup $\langle \gamma_0 \rangle \subset \mathrm{PSL}_2(\mathbb{F}_p)$ of order 6. But then $\gamma_0 \in 3A$ or $(-\gamma_0) \in 3A$ and so $2A \subset (3A)^\mathbb{Z}$ or $2A \subset (-3A)^\mathbb{Z}$ – a contradiction.

However pA and pB are not very different and criterion 2.6 cannot be applied directly. We use instead the following argument. Assume there is a k -regular extension $F/k(T)$ such that $F\mathbb{C}/\mathbb{C}(T)$ specializes to $L_1\mathbb{C}/\mathbb{C}(T)$ and $L_2\mathbb{C}/\mathbb{C}(T)$. From above we have $r_F = 3$ and, for $\mathbf{C}_F = (C_1, C_2, C_3)$, there should exist integers $a_i, b_i, c_i \in \mathbb{Z}$, $i = 1, 2$, such that $(C_1^{a_1}, C_2^{b_1}, C_3^{c_1}) = (2A, pA, pB)$ and $(C_1^{a_2}, C_2^{b_2}, C_3^{c_2}) = (3A, pA, pB)$. Necessarily $C_2, C_3 \in \{pA, pB\}$, $2A \subset C_1^\mathbb{Z}$ and $3A \subset C_1^\mathbb{Z}$. This contradicts $2A \# 3A$.

Finally take $G = M$ the Fischer-Griess Monster. We will use two known \mathbb{Q} -regular realizations $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$ of G , for which $r_{L_1} = r_{L_2} = 3$ and

$$\mathbf{C}_{L_1} = (2A, 3B, 29A) \text{ and } \mathbf{C}_{L_2} = (2A, 3C, 38A)$$

(where we use the standard notation from the Atlas of simple groups for the conjugacy classes of M). The extension $L_1/\mathbb{Q}(T)$ is the one originally produced by J. Thompson [Tho84]; the main point is that \mathbf{C}_{L_1} is a “rigid triple”. Computer programs now exist to find other rigid tuples. The triple \mathbf{C}_{L_2} was communicated to me by J. Koenig who checked that it is rigid, assuming that the current classification of all (certain and hypothetical) maximal subgroups of M is correct.

Assume there is a k -regular extension $F/k(T)$ such that $F\mathbb{C}/\mathbb{C}(T)$ specializes to $L_1\mathbb{C}/\mathbb{C}(T)$ and $L_2\mathbb{C}/\mathbb{C}(T)$. Then we have $r_F = 3$. Set $\mathbf{C}_F = (C_1, C_2, C_3)$. From the Atlas of simple groups, there is only one conjugacy class, $38A$, whose elements are of order a multiple of 38 (and this multiple is 38) and there are three conjugacy classes, $29A$, $87A$ and $87B$, whose elements are of order a multiple of 29 (and these multiples are 29, 87 and 87). One of C_1, C_2, C_3 , say C_1 , must be $38A$ and one, say C_2 , should be $29A$ or $87A$ or $87B$. Furthermore $3B$ and $3C$ are not a power of $87A$ or $87B$. This leads to these possibilities for the triple \mathbf{C} of ramification indices of $F/\mathbb{Q}(T)$:

$$\mathbf{C} = (38A, 29A, C_3) \text{ or } \mathbf{C} = (38A, 87A, C_3) \text{ or } \mathbf{C} = (38A, 87B, C_3)$$

with C_3 of order divisible by 3. But then the lower bound for the number r_{T_0} of branch points of a specialization $F_{T_0}/\mathbb{Q}(T)$ with $T_0 \in \mathbb{Q}(T)$ given in theorem 3.1 (b-1) gives $r_{T_0} > 3$ and so neither $L_1/\mathbb{Q}(T)$

nor $L_2/\mathbb{Q}(T)$ can be a specialization of an extension $F/\mathbb{Q}(T)$ with inertia canonical invariant \mathbf{C} . \square

2.4. Non \mathbb{Q} -parametric extensions $F/\mathbb{Q}(T)$. Assume that k is a number field.

2.4.1. Main tool for producing non k -parametric extensions $F/k(T)$.

Theorem 2.11. *Let $F/k(T)$ and $L/k(T)$ be two k -regular Galois extensions with respective groups G and H such that $H \subset G$. There exist polynomials $\tilde{P}_1, \dots, \tilde{P}_N \in k[U, T, Y]$ with the following properties:*

- (a) *\tilde{P}_i is monic in Y , $\deg_Y(\tilde{P}_i) = |G|$ and the splitting field over $\overline{k(U)}(T)$ of \tilde{P}_i is the extension $F\overline{k(U)}/\overline{k(U)}(T)$, $i = 1, \dots, N$,*
- (b) *For every field K with $k \subset K \subset \mathbb{C}(U)$, for all $u_0 \in K$ but finitely many in \bar{k} , and for all $t_0 \in K$ not a branch point of $F/k(T)$, the specialization L_{u_0}/K is K -isomorphic to the specialization F_{t_0}/K iff for some $i \in \{1, \dots, N\}$, there exists $y_0 \in K$ such that $\tilde{P}_i(u_0, t_0, y_0) = 0$.*

Theorem 2.11 is proved in §4.

2.4.2. The working hypothesis. We will deduce some non k -parametric conclusions from theorem 2.11 under this “working hypothesis”:

(WH) *Given a number field k and polynomials $P_1, \dots, P_N \in k[U, T, Y]$ irreducible in $\bar{k}[U, T, Y]$, we have the following: if none of the equations $P_i(U, t, y) = 0$ has a solution $(T_0, Y_0) \in \mathbb{C}(U)^2$, then for infinitely many $u_0 \in k$, none of the equations $P_i(u_0, t, y) = 0$ has a solution $(t_0, y_0) \in k^2$ ($i = 1, \dots, N$).*

We comment on this hypothesis below in §2.4.4.

2.4.3. Main conclusions. We first explain how we combine our working hypothesis and theorem 2.11.

Proposition 2.12. *Assume (WH) holds and let k be a number field and $F/k(T)$ be a k -regular Galois extension of group G .*

- (a) *If a k -regular Galois extension $L/k(U)$ of group $H \subset G$ is such that $L\mathbb{C}/\mathbb{C}(U)$ is not a specialization of $F/k(T)$ at any $T_0 \in \mathbb{C}(U)$, there are infinitely many $u_0 \in k$ such that the specialization L_{u_0}/k of $L/k(U)$ is not a specialization of $F/k(T)$ at any unbranched $t_0 \in k$.*
- (b) *If $F/k(T)$ is k -parametric then it is weakly $k(U)$ -parametric.*
- (c) *Every group with no weakly $k(U)$ -parametric extension has no k -parametric extension.*

Corollary 2.13. *Assume (WH) holds and let k be a number field. Every group as in corollary 2.10 has no k -parametric extension.*

Proof of proposition 2.12. Let $F/k(T)$ and $L/k(U)$ be as in (a) and $\tilde{P}_1, \dots, \tilde{P}_N$ be the polynomials provided by theorem 2.11. From this result and the assumption in (a), none of the equations $\tilde{P}_i(U, t, y) = 0$ has a solution $(T_0, Y_0) \in \mathbb{C}(U)^2$, $i = 1, \dots, N$. Under (WH), one may conclude that for infinitely many $u_0 \in k$, none of the equations $\tilde{P}_i(u_0, t, y) = 0$ has a solution $(t_0, y_0) \in k^2$. From theorem 2.11, for these u_0 , the specialization L_{u_0}/k , which is of Galois group contained in G , is not a specialization F_{t_0}/k of $F/k(T)$ with $t_0 \in k$. Statements (b) and (c) follow straightforwardly from (a). \square

Remark 2.14. (a) The proof shows that proposition 2.12 and corollary 2.13 still hold if (WH) is replaced by the weaker hypothesis (WH-Gal/ \mathbb{C}) for which the conclusion of (WH) solely holds for polynomials P_1, \dots, P_n such that

- $P_i(U, T, Y)$ is irreducible in $\overline{k(U)}[T, Y]$, $i = 1, \dots, N$,
- the splitting field over $\overline{k(U)}(T)$ of \tilde{P}_i is the extension $\overline{Fk(U)}/\overline{k(U)}(T)$, that is, this splitting field is $\overline{k(U)}(T)$ -isomorphic to $\overline{Fk(U)}$, $i = 1, \dots, N$.

(b) We can now explain how, conditionally, Legrand's result (mentioned in §1.1) can be deduced from ours. Assuming G is the group of some \mathbb{Q} -regular Galois extension $L/\mathbb{Q}(U)$, if $F/\mathbb{Q}(T)$ is another \mathbb{Q} -regular Galois extension of group G such that $LC/\mathbb{C}(U)$ is not a $\mathbb{C}(U)$ -specialization of $F/\mathbb{Q}(T)$, then it follows from proposition 2.12 that, if G satisfies (WH-Gal/ \mathbb{C}), $F/\mathbb{Q}(T)$ is not \mathbb{Q} -parametric.

For example, one can take for $F/\mathbb{Q}(T)$ a specialization $L_{U_0}/\mathbb{Q}(T)$ with $U_0(T) = a + T^5$ with $a \in \mathbb{Q}$. For all but finitely many $a \in \mathbb{Q}$, $\text{Gal}(F/\mathbb{Q}(T)) = G$. From inequality (*) from §2.1.1, the branch point number of $FC/\mathbb{C}(T)$ is bigger than that of $LC/\mathbb{C}(U)$. From theorem 2.1, the latter is not a specialization of the former with $T_0 \in \mathbb{C}(U)$.

2.4.4. Comments on the working hypothesis.

(a) The working hypothesis (WH) is known to hold in these situations:

- $\deg_T(P) = 0$: (WH) is then Hilbert's Irreducibility Theorem; (WH) is an extension of HIT to 2-indeterminate polynomials.

- the affine $\overline{k(U)}$ -curve of equation $P(U, t, y) = 0$ is of genus 0. This follows from Schinzel's thm 38 in [Sch82]. A stronger conclusion even holds: the infinitely many u_0 can be chosen in the ring of integers of k .
- the polynomial $P(U, T, Y)$ is of the form $Y^n - U^m Q(T)$ with $n \geq 2$ dividing $\deg(Q)$, m relatively prime to n and $Q \in k[T] \setminus k$ a polynomial with integral coefficients such that the Galois group of Q has an element that fixes no root of Q (e.g. Q is irreducible in $k[T]$) [Leg16b].

(b) There is no known counter-example to (WH). In this context, Cassels and Schinzel [CS82] consider the family of genus 1 curves $y^2 = t(t^2 - (7 + 7U^4)^2)$ and show that this equation has no solution $(T_0(U), Y_0(U)) \in \mathbb{Q}(U)^2$ and that, under a conjecture of Selmer [Sel54], for every $u_0 \in \mathbb{Q}$, the equation $y^2 = t(t^2 - (7 + 7u_0^4)^2)$ has a solution $(t_0, y_0) \in \mathbb{Q}^2$. This however does not provide a counter-example (even conjectural) to (WH) as the equation $y^2 = t(t^2 - (7 + 7U^4)^2)$ also has solutions in $\mathbb{C}(U)$.

(c) While it may be hard to find a non k -parametric extension $F/k(T)$ to test the working hypothesis, it is possible to produce extensions $L/k(U)$ and $F/k(T)$ with the former not a specialization of the latter (for example do as above in (b)). The polynomials $\tilde{P}_1, \dots, \tilde{P}_N$ given by theorem 2.11 then are good candidates to test the working hypothesis.

3. $\mathbb{C}(U)$ -SPECIALIZATIONS OF GALOIS EXTENSIONS $F/\mathbb{C}(T)$

Let $F/\mathbb{C}(T)$ be a degree d Galois extension of group G , with r branch points t_1, \dots, t_r , inertia canonical invariant $\mathbf{C} = (C_1, \dots, C_r)$ and associated ramification indices $\mathbf{e} = (e_1, \dots, e_r)$. Also set

$$\begin{cases} \varepsilon = \frac{1}{e_1} + \dots + \frac{1}{e_r} \\ e_\infty = \max(e_1, \dots, e_r) \end{cases}$$

Let $T_0(U) = a(U)/b(U) \in \mathbb{C}(U) \setminus \mathbb{C}$ with $a, b \in \mathbb{C}[U]$ relatively prime and $b \neq 0$. Set

$$N = \deg(T_0) = \max(\deg(a), \deg(b))$$

We will compare the invariants of $F/\mathbb{C}(T)$ to those of $F_{T_0}/\mathbb{C}(T)$.

Note that when $N = 1$, T_0 is a linear fractional transformation and the two extensions $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are isomorphic. More specifically, T_0 interprets as an automorphism of $\mathbb{P}^1(\mathbb{C})$ and if $f : X \rightarrow \mathbb{P}^1$ is the branched cover corresponding to $F/\mathbb{C}(T)$, then $F_{T_0}/\mathbb{C}(T)$ corresponds to the cover $f \circ T_0^{-1}$. In particular the invariants G, r, d, g, \mathbf{C} are the same for the two extensions.

3.1. Invariants of the specialized extensions. Denote the invariants of the specialized extensions $F_{T_0}/\mathbb{C}(U)$ by $G_{T_0}, d_{T_0} = |G_{T_0}|, g_{T_0}$ and \mathbf{C}_{T_0} . The following statement is the most precise of this section. We will in particular deduce theorem 2.1 from it.

Theorem 3.1. *Consider the specialized extension $F_{T_0}/\mathbb{C}(U)$.*

(a) *We have $G_{T_0} \subset G$, equivalently $d_{T_0} \leq d$. Furthermore $d_{T_0} < d$ if and only if there is a subfield $L \subset F$, $L \neq \mathbb{C}(T)$, of genus 0, such that a specialization of it at T_0 is trivial: $L_{T_0} = \mathbb{C}(U)$.*

(b) The branch point number r_{T_0} satisfies $r_{T_0} \leq rN$ and

$$(b-1) \quad r_{T_0} \geq \frac{(r - \varepsilon - 2)N + 2}{1 - (1/e_\infty)} \quad \text{if } r \geq 0$$

$$(b-2) \quad r_{T_0} \geq (r - 4)N + 4 \quad \text{if } r \geq 4$$

(c) The inertia canonical invariant \mathbf{C}_{T_0} of $F_{T_0}/\mathbb{C}(U)$ consists of conjugacy classes in G_{T_0} of powers g^α ($\alpha \in \mathbb{N}$) of elements of $C_1 \cup \dots \cup C_r$.

(d) The genus g_{T_0} satisfies $g_{T_0} \leq N(g + d - 1)$, and, if $G_{T_0} = G$,

$$g_{T_0} - g \geq \frac{d}{4}(N - 1)(r - 4)$$

Remark 3.2. The lower and upper bounds for g_{T_0} in (d) are better than those that can be deduced from inequalities (b-1) or (b-2) by combining them with the usual ones given by Riemann-Hurwitz:

$$\frac{r}{2} + 1 - n \leq g \leq \frac{rn}{2} + 1 - n - \frac{r}{2}$$

Proof. (a) The first part of (a) is standard.

Assume that there is a subfield $L \subset F$, $L \neq \mathbb{C}(T)$ with a trivial specialization: $L_{T_0} = \mathbb{C}(U)$. Then we have

$$d_{T_0} = [F_{T_0} : L_{T_0}] [L_{T_0} : \mathbb{C}(U)] \leq [F : L] < d.$$

For the converse, assume that $d_{T_0} < d$. A standard argument (e.g. [FJ04, lemma 13.1.2]) from the theory of hilbertian fields (applied here to the field $\mathbb{C}(U)$) shows that there exists $\theta \in F \setminus \mathbb{C}(T)$ such that $\mathbb{C}(T, \theta)_{T_0} = \mathbb{C}(U)$: if $P(T, Y)$ is an affine equation of $F/\mathbb{C}(T)$, θ is a coefficient in $\overline{\mathbb{C}(T)}$ of a factorisation $P(T, Y)$ in $\overline{\mathbb{C}(T)}[Y]$. The field $L = \mathbb{C}(T, \theta)$ is the desired field.

That L is of genus 0 follows from $L_{T_0} = \mathbb{C}(U)$. Indeed, if $Q(T, Y)$ is an affine equation for $L/\mathbb{C}(T)$, $L_{T_0} = \mathbb{C}(U)$ means that there exists $Y_0(U) \in \mathbb{C}(U)$ such that $Q(T_0(U), Y_0(U)) = 0$, which is a rational parametrization of the curve of equation $Q(T, Y)$. Hence its function field L is of genus 0.

(b) A first point of the proof is that

(*) if $u \in \mathbb{P}^1(\mathbb{C})$ is a branch point of $F_{T_0}/\mathbb{C}(U)$, there exists a branch point t_i of $F/\mathbb{C}(T)$ such that $T_0(u) = t_i$ and, conversely, if $T_0(u) = t_i$, the associated inertia group is generated by some power g_i^α ($\alpha \in \mathbb{N}$) of an element $g_i \in C_i$.

This statement, which in particular yields conclusion (c), follows from the Specialization Inertia Theorem (SIT) recalled in §5. More specifically, we use it in the situation that the Dedekind domain is $A = \mathbb{C}[U]$

(or $A = \mathbb{C}[1/U]$ for $u = \infty$), the K -regular extension is $F\mathbb{C}(U)/\mathbb{C}(U)(T)$ and \mathfrak{p} is the ideal $\mathfrak{p} = \langle U - u \rangle$ if $u \in \mathbb{C}$ (and $\mathfrak{p} = \langle 1/U \rangle$ if $u = \infty$).

A few remarks on the assumptions from §5 are in order:

- (1) $|G| \notin \mathfrak{p}$ since $A/\mathfrak{p} = \mathbb{C}$ is of characteristic 0.
- (2) *there is no vertical ramification at \mathfrak{p} in the extension $FK/K(T)$* : indeed if \mathcal{Y} is a primitive element of $F/\mathbb{C}(T)$, integral over A , then $1, \mathcal{Y}, \dots, \mathcal{Y}^{d-1}$ (with $d = |G|$) are integral over A and over $A[T]$ as well, and form a $K(T)$ -basis of $F\mathbb{C}(U)/\mathbb{C}(U)(T)$. The discriminant of this basis is a non-zero element of $\mathbb{C} \subset A$, and so remains non-zero modulo \mathfrak{p} . This classically guarantees the content of our claim.
- (3) *no two different branch points of $F/K(T)$ meet modulo \mathfrak{p}* : indeed the branch points are those of $F/\mathbb{C}(T)$ and their mutual differences $t_i - t_j$ or $(1/t_i) - (1/t_j)$ are non-zero elements of $\mathbb{C} \subset A$ and remain non-zero modulo \mathfrak{p} .
- (4) *the ideal \mathfrak{p} is unramified in $K(t_1, \dots, t_r)/K = \mathbb{C}(U)/\mathbb{C}(U)$* .
- (5) *t_i and $1/t_i$ are integral over $\tilde{A}_{\mathfrak{p}}$: $t_i, 1/t_i \in \mathbb{C} \cup \{\infty\}$ $i = 1, \dots, r$.*

The SIT concludes that if $u \in \mathbb{P}^1(\mathbb{C})$ is a branch point of $F_{T_0}/\mathbb{C}(U)$, there exists $i \in \{1, \dots, r\}$ such that T_0 meets t_i modulo \mathfrak{p} , which exactly means that $T_0(u) = t_i$, and, secondly, that, if $T_0(u) = t_i$, the inertia group of $F_{T_0}/\mathbb{C}(U)$ at u , is generated by an element of C_i^α with

$$(**) \quad \alpha = \text{ord}_u(T_0(U) - t_i)$$

This concludes the proof of (*). To simplify the exposition of the rest of the proof, we first assume:

(H) *neither ∞ nor $T_0(\infty)$ is a branch point of $F/\mathbb{C}(T)$* .

and will explain afterwards how to reduce to this hypothesis.

For an element $u \in \mathbb{P}^1(\mathbb{C})$ such that $T_0(u) = t_i$ for some $i = 1, \dots, r$ to be a branch point of $F_{T_0}/\mathbb{C}(U)$, the integer α from (**) should not be a multiple of e_i . Note further that because of (H), $u \neq \infty$ and u is not a pole of T_0 .

For each $i = 1, \dots, r$, label the roots in \mathbb{C} of $a(U) - t_i b(U)$ as follows:

- u_{i1}, \dots, u_{ip_i} are the p_i distinct simple roots,
- v_{i1}, \dots, v_{iq_i} are the q_i distinct multiple roots of orders, say m_{i1}, \dots, m_{iq_i} , non divisible by e_i ,
- w_{i1}, \dots, w_{is_i} are the s_i distinct multiple roots of orders, say n_{i1}, \dots, n_{is_i} , divisible by e_i .

Then we have

$$(1) \quad p_i + \sum_{j=1}^{q_i} m_{ij} + \sum_{j=1}^{s_i} n_{ij} = N, \quad i = 1, \dots, r,$$

$$(2) \sum_{i=1}^r \left(\sum_{j=1}^{q_i} (m_{ij} - 1) + \sum_{j=1}^{s_i} (n_{ij} - 1) \right) \leq 2N - 2.$$

Equality (1) is clear. As to (2), it follows from the fact (left to the reader⁹) that if $u \in \mathbb{C}$ is root of $a(U) - t_i b(U)$ of order $m \geq 1$ for some $i = 1, \dots, r$, then u is a root of order $m - 1$ of the polynomial $a'b - ab'$, which is of degree $2N - 2$. An alternate argument consists in applying the Riemann-Hurwitz formula to the branched cover $T_0 : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ induced by the rational function $T_0(U)$: the left-hand side term from (2) is smaller than or equal to the term $\sum_P (e_P - 1)$ of this formula (where P ranges over all ramified points) and so is $\leq 2 \cdot 0 - 2 + 2 \deg(T_0) = 2N - 2$.

Statement (*) gives

$$r_{T_0} = \sum_{i=1}^r (p_i + q_i)$$

Clearly $r_{T_0} \leq rN$ follows. Inequality (2), conjoined with (1), rewrites

$$\sum_{i=1}^r (N - p_i - q_i - s_i) \leq 2N - 2$$

so we obtain

$$(***) \quad r_{T_0} \geq (r - 2)N + 2 - \sum_{i=1}^r s_i$$

From (1), for $i = 1, \dots, r$, we also have $p_i + q_i + e_i s_i \leq N$, whence

$$s_i \leq \frac{N}{e_i} - \frac{p_i + q_i}{e_i}$$

The definition of e_∞ and ε leads to

$$r_{T_0} \geq rN - (2N - 2) - \varepsilon N + \frac{1}{e_\infty} \sum_{i=1}^r (p_i + q_i)$$

and finally to inequality (b-1).

From (2) we can also deduce that

$$\sum_{i=1}^r s_i \leq 2N - 2$$

which conjoined with (***), yields inequality (b-2).

(d) Write the Riemann-Hurwitz formula for $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(U)$:

⁹with this hint: if $a^{(k)}(u) - t_i b^{(k)}(u) = 0$ for $k = 0, \dots, m - 1$, then $a^{(h)}(u)b^{(k)}(u) - a^{(k)}(u)b^{(h)}(u) = 0$ for $h, k = 0, \dots, m - 1$. The claim follows from the observation that every derivative $(a'b - ab')^{(h)}$ ($h = 0, \dots, m - 2$) is a sum of terms of the form $a^{(h)}b^{(k)} - a^{(k)}b^{(h)}$ with $h, k = 0, \dots, m - 1$.

$$\begin{cases} 2g - 2 = -2d + \sum_F (e_{\mathcal{P}} - 1) \\ 2g_{T_0} - 2 = -2d_{T_0} + \sum_{F_{T_0}} (e_{\mathcal{P}} - 1) \end{cases}$$

where \sum_F (resp. $\sum_{F_{T_0}}$) means that the sum ranges over all places of F (resp. of F_{T_0}) trivial on \mathbb{C} . The first claim from (d) comes from

$$g_{T_0} = 1 - d_{T_0} + \frac{1}{2} \sum_{F_{T_0}} (e_{\mathcal{P}} - 1) \leq \frac{N}{2} \sum_F (e_{\mathcal{P}} - 1) = N(g - 1 + d)$$

As $F/\mathbb{C}(T)$ is Galois, we also have

$$\sum_F (e_{\mathcal{P}} - 1) = \sum_{i=1}^r \sum_{\mathcal{P}/t_i} (e_i - 1) = \sum_{i=1}^r \left(d - \frac{d}{e_i} \right)$$

Assume $G_{T_0} = G$, so $d_{T_0} = d$. Our analysis of the branch points of the specialized extension $F_{T_0}/\mathbb{C}(U)$ yields:

$$\sum_{F_{T_0}} (e_{\mathcal{P}} - 1) \geq \sum_{i=1}^r \left(d - \frac{d}{e_i} \right) p_i$$

whence

$$g_{T_0} - g \geq \frac{1}{2} \sum_{i=1}^r \left(d - \frac{d}{e_i} \right) (p_i - 1)$$

Now we have, for each $i = 1, \dots, r$,

$$\begin{aligned} p_i &= N - \sum_{j=1}^{q_i} m_{ij} - \sum_{j=1}^{s_i} n_{ij} \\ &\geq N - 2 \left(\sum_{j=1}^{q_i} (m_{ij} - 1) + \sum_{j=1}^{s_i} (n_{ij} - 1) \right) \end{aligned}$$

We deduce:

$$\begin{aligned} g_{T_0} - g &\geq \frac{1}{2} \sum_{i=1}^r \left(d - \frac{d}{e_i} \right) \left(N - 1 - 2 \left(\sum_{j=1}^{q_i} (m_{ij} - 1) + \sum_{j=1}^{s_i} (n_{ij} - 1) \right) \right) \\ &\geq \frac{d}{4} (r(N - 1) - 2(2N - 2)) \\ &= \frac{d}{4} (N - 1)(r - 4) \end{aligned}$$

Finally we explain how to reduce to a situation for which assumption (H) is satisfied. Note first that the parameters r, d, g, \mathbf{C} are unchanged if the extension $F/\mathbb{C}(T)$ is replaced by any extension $F_{\chi}/\mathbb{C}(T)$ with $\chi \in \mathbb{C}(T)$ of degree 1.

For some fixed $\theta_0 \in \mathbb{C} \setminus \{t_1, \dots, t_r\}$, consider the linear fractional transformation χ defined by

$$\chi^{-1}(T) = \frac{\tau T + \mu}{T - \theta_0}$$

where τ, μ are chosen in \mathbb{C} so that the complex numbers $\chi^{-1}(t_1), \dots, \chi^{-1}(t_r)$ are different from ∞ ; such a choice is possible as \mathbb{C} is infinite. These r complex numbers are the branch points of the extension $F_\chi/\mathbb{C}(T)$, and so these branch points are different from ∞ . Fix then a second linear fractional transformation χ' such that $T_0(\chi'(\infty)) \notin \{t_1, \dots, t_r\}$. By construction the extension $F_\chi/\mathbb{C}(T)$ and the rational function $\chi^{-1} \circ T_0 \circ \chi'$ satisfy the assumption (H). Therefore the conclusions from theorem 3.1 comparing the ramification invariants of the specialized extension

$$(F_\chi)_{\chi^{-1} \circ T_0 \circ \chi'} / \mathbb{C}(U) = F_{T_0 \circ \chi'} / \mathbb{C}(U)$$

with those of $F_\chi/\mathbb{C}(T)$ are satisfied. These conclusions hold as well for the invariants of the specialized extension $F_{T_0}/\mathbb{C}(U)$ compared to those of $F/\mathbb{C}(T)$ since $F_{T_0}/\mathbb{C}(U)$ (resp. $F/\mathbb{C}(T)$) is obtained from $F_{T_0 \circ \chi'}/\mathbb{C}(U)$ (resp. $F_\chi/\mathbb{C}(T)$) by composition with an automorphism of $\mathbb{C}(U)$ (resp. an automorphism of $\mathbb{C}(T)$). \square

In the next subsections, we explain how to theorem 2.1 can be deduced from theorem 3.1.

3.2. Proof of theorem 2.1(a). Assume $g \geq 1$ and let $L/\mathbb{C}(T)$ be a Galois extension such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$, *i.e.*, there exists $T_0 \in \mathbb{C}(U) \setminus \mathbb{C}$ such that $L/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$. As in §3.1 denote the invariants of $F_{T_0}/\mathbb{C}(T)$ by $G_{T_0}, r_{T_0}, g_{T_0}, \mathbf{C}_{T_0}$.

We already know that $G \supset G_{T_0}$ and $\mathbf{C} \prec \mathbf{C}_{T_0}$ (theorem 3.1 (a),(c)).

Next we show that $r_{T_0} \geq r$. We may assume that $N \geq 2$.

A first case is when $r \geq 4$: $r_{T_0} \geq r$ follows from theorem 3.1 (b-2).

From theorem 3.1 (b-1), if $\varepsilon \leq (r-1)/2$ and $r \geq 3$ we have:

$$r_{T_0} > \left(r - \frac{r-1}{2} - 2\right)N + 2 \geq 2\left(\frac{r}{2} - \frac{3}{2}\right) + 2 = r - 1$$

In particular, for $r = 3$, we have $r_{T_0} \geq r$ if $\varepsilon \leq 1$. A simple check shows that the following 3-tuples \mathbf{e} :

$$(2, 2, 2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 2, e), (e \geq 3)$$

are exactly those for which $\varepsilon > 1$ and that $g = 0$ in these cases.

We are left with the case $r = 2$. But then $F/\mathbb{C}(T)$ is a cyclic extension with two branch points and hence $g = 0$. This ends the proof of the inequality $(G, r, \mathbf{C}) \prec (G_{T_0}, r_{T_0}, \mathbf{C}_{T_0})$ when $g \geq 1$.

Assume next $G_{T_0} = G$. The above inequality then also holds if $g = 0$. The only non-trivial point is $r_{T_0} \geq r$. We know that $r_{T_0} < r$ possibly happens only when $r \leq 3$ and $g = 0$ and in this case $r_{T_0} < r$ means that either $r_{T_0} = 0$ in which case $F_{T_0} = \mathbb{C}(T)$ and then $G_{T_0} = \{1\} \neq G$, or, $r_{T_0} = 2$ in which case $F_{T_0}/\mathbb{C}(T)$ is cyclic, and then again $G_{T_0} \neq G$. Indeed, in this last case, G cannot be cyclic as $r = 3$, $g = 0$ and a cyclic group has no generating set $\{g_1, g_2, g_3\}$ such that $g_1 g_2 g_3 = 1$ and with respective orders those in one of the above triples \mathbf{e} . Finally it immediately follows from theorem 3.1 (d) that $g_{T_0} \geq g$ if $r \geq 4$.

Remark 3.3. If F is of genus 0 and $G_{T_0} \neq G$, $r_{T_0} < r$ may happen. One may then have $G_{T_0} = \{1\}$ or not (see example 3.3.2).

3.3. The exceptional genus 0 cases. The Riemann-Hurwitz formula

$$2g - 2 = -2d + \sum_{i=1}^r (e_i - 1) \frac{d}{e_i} \quad \text{where } d = |G|,$$

in a Galois situation yields

$$2g - 2 = d(r - 2 - \varepsilon)$$

As $\varepsilon \leq r/2$ we have $2g - 2 \geq d(\frac{r}{2} - 2)$, and if $\varepsilon \leq (r - 1)/2$, then

we have $2g - 2 \geq \frac{d}{2}(r - 3)$. Hence if $g = 0$, $r \leq 3$ and $\varepsilon > 1$.

Conclude that if $g = 0$ we necessarily are in one of these cases:

- (1) $r = 3$ and $\mathbf{e} \in \{(2, 2, 2), (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 2, n), (n \geq 3)\}$
with corresponding groups $(\mathbb{Z}/2\mathbb{Z})^2$, A_4 , S_4 , A_5 , D_{2n} ($n \geq 3$).
- (2) $r = 2$ then $F/\mathbb{C}(T)$ is a cyclic extension with 2 branch points.

Namely, a simple calculation shows that the tuples \mathbf{e} are the indicated ones. Concerning the corresponding groups, note first that, as F is of genus 0, G must be a subgroup of $\text{PGL}_2(\mathbb{C})$ and so one of the proposed list. The case $r = 2$ is clear. Assume $r = 3$. Then G cannot be cyclic. For $\mathbf{e} = (2, 2, 2)$, G is generated by two involutions with product an involution, so $G = (\mathbb{Z}/2\mathbb{Z})^2$. Similarly one obtains D_{2n} (dihedral group of order $2n$) if $\mathbf{e} = (2, 2, n)$ ($n \geq 3$). If $\mathbf{e} = (2, 3, 4)$ G must be S_4 as it cannot be any of the others. We obtain similarly that $G = A_4$ if $\mathbf{e} = (2, 3, 3)$ and $G = A_5$ if $\mathbf{e} = (2, 3, 5)$.

Next we show that in all these cases, if r distinct points $t_1, \dots, t_r \in \mathbb{P}^1(\mathbb{C})$ are fixed ($r = 2$ or $r = 3$), there is one and only one Galois extension $F/\mathbb{C}(T)$ of group G , ramification indices $\mathbf{e} = (e_1, \dots, e_r)$ and branch points t_1, \dots, t_r . Furthermore, as PGL_2 is 3-transitive on $\mathbb{P}^1(\mathbb{C})$, up to isomorphism, there is exactly one extension $F/\mathbb{C}(T)$ in each case.

From corollary 4.2, this unique extension $F/\mathbb{C}(T)$ of group G in each case is $\mathbb{C}(U)$ -parametric.

Concerning uniqueness, one checks first that up to some (anti-)isomorphism of G (which does not change the Galois extension $F/\mathbb{C}(T)$), there is, for each r -tuple \mathbf{e} , a unique possible r -tuple $\mathbf{C} = (C_1, \dots, C_r)$ and second, that this r -tuple is *rigid*, that is: there is a unique r -tuple $(g_1, \dots, g_r) \in C_1 \times \dots \times C_r$ such that $\langle g_1, \dots, g_r \rangle = G$ and $g_1 \cdots g_r = 1$, up to componentwise conjugation by an element of G . It then classically follows from the Riemann Existence Theorem that there is one and only one Galois extension $F/\mathbb{C}(T)$ as desired if in addition the branch points are fixed.

Below we produce in each case an example of an extension $F/\mathbb{C}(T)$ with the given invariants.

3.3.1. $r = 2$, $G = \mathbb{Z}/d\mathbb{Z}$ with $d \geq 1$: $\mathbb{C}(\sqrt[d]{T})/\mathbb{C}(T)$ is a Galois extension of group $\mathbb{Z}/d\mathbb{Z}$ branched at 0 and ∞ with ramification indices d .

3.3.2. $\mathbf{e} = (2, 2, 2)$, $G = (\mathbb{Z}/2\mathbb{Z})^2$: for $F = \mathbb{C}(\sqrt{T}, \sqrt{T-1})$, $F/\mathbb{C}(T)$ is a Galois extension of group $(\mathbb{Z}/2\mathbb{Z})^2$. A primitive element of $F/\mathbb{C}(T)$ is for example $\sqrt{T} + \sqrt{T-1}$. An affine equation is the polynomial $Y^4 + 2(1-2T)Y^2 + 1$. There are three branch points: 0, 1 and ∞ , which all are of index 2. For $T_0 = T^2$, we have $F_{T_0} = \mathbb{C}(T, \sqrt{T^2-1})$ whose branch points are 1 and -1 .

For the other cases, we produce a generating set of G of 3 elements g_1, g_2, g_3 of orders e_1, e_2, e_3 and such that $g_1 g_2 g_3 = 1$.

3.3.3. $\mathbf{e} = (2, 3, 3)$, $G = A_4$: take

$$g_1 = (1\ 2)(3\ 4), g_2 = (1\ 2\ 3), g_3 = (2\ 3\ 4)$$

3.3.4. $\mathbf{e} = (2, 3, 4)$, $G = S_4$: take

$$g_1 = (1\ 2), g_2 = (2\ 3\ 4), g_3 = (4\ 3\ 2\ 1)$$

(The conjugacy classes of g_1, g_2, g_3 in S_4 being “rational”, a standard argument shows further that, if one fixes the three branch points in $\mathbb{P}^1(\mathbb{Q})$, the unique corresponding extension $F/\mathbb{C}(T)$ is defined over \mathbb{Q}).

3.3.5. $\mathbf{e} = (2, 3, 5)$, $G = A_5$: take

$$g_1 = (1\ 5)(3\ 4), g_2 = (1\ 2\ 4), g_3 = (5\ 4\ 3\ 2\ 1)$$

3.3.6. $\mathbf{e} = (2, 2, n)$, $e \geq 3$, $G = D_{2n}$: take g_1, g_2 two involutions with $g_1 g_2 = g_3^{-1}$ generating the normal cyclic subgroup. For n odd, an explicit example is the Galois extension $F/\mathbb{C}(T)$ with affine equation $Y^{2n} - TY^n + 1$ which is branched at 2, -2 , ∞ with ramification indices 2, 2 and n . As it is $\mathbb{C}(U)$ -parametric, it follows from the uniqueness

conclusion of theorem 2.1 (b) that it is isomorphic to the Hashimoto-Mihake generic extension for D_{2n} mentioned in remark 2.5.

3.4. Theorem 2.1 (b).

3.4.1. *A preliminary lemma.* Retain the notation already introduced for theorem 2.1 (a).

Lemma 3.4. *When $N = \deg(T_0) > 1$, we have $r_{T_0} > r$ in each of the following cases:*

- (a) $r \geq 5$,
- (b) $F \neq \mathbb{C}(T)$ and $\varepsilon \leq (r-2)/2$,
- (c) $N \geq 4$, $r = 4$ and $\varepsilon \leq 3/2$,
- (d) $N \geq 4$, $r = 3$ and $\varepsilon \leq 3/4$.

Proof. Assume $N > 1$. If $r \geq 5$ as in (a), theorem 3.1 (b-2) gives

$$r_{T_0} \geq (r-4)N + 4 \geq 2r - 4 > r$$

From theorem 3.1 (b-1), we have

$$(*) \quad r_{T_0} > (r - \varepsilon - 2)N + 2$$

Under the assumptions of (b), we deduce

$$r_{T_0} > \left(\frac{r}{2} - 1\right)N + 2 \geq \left(\frac{r}{2} - 1\right)2 + 2 = r$$

Finally $r_{T_0} > r$ easily follows from (*) above in the last two cases (c) and (d). \square

3.4.2. *Proof of theorem 2.1 (b).* The only non-trivial point is the antisymmetry of \prec . Let $F/\mathbb{C}(T)$ and $F'/\mathbb{C}(T)$ be two non-isomorphic extensions in the set \mathcal{E}^* such that $F/\mathbb{C}(T) \prec F'/\mathbb{C}(T)$ and $F'/\mathbb{C}(T) \prec F/\mathbb{C}(T)$. Let $T_0, T'_0 \in \mathbb{C}(T)$ such that $F'/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$ and $F/\mathbb{C}(T) = F'_{T'_0}/\mathbb{C}(T)$ with $\deg(T_0) \geq 2$ and $\deg(T'_0) \geq 2$. From theorem 2.1 (a), $F/\mathbb{C}(T)$ and $F'/\mathbb{C}(T)$ have the same group G , the same branch point number r , the same inertia canonical invariant \mathbf{C} and the same ramification indices \mathbf{e} . We also have $F_{T_0 T'_0}/\mathbb{C}(T) = F/\mathbb{C}(T)$.

Recall that $F/\mathbb{C}(T) \in \mathcal{E}^*$ means one of the following situations holds:

- (a) G is of rank ≥ 4 ,
- (b) G is of rank 3 and of odd order,
- (c) G is of rank 2 and order non divisible by 2 or 3,
- (d) F is of genus $g = 0$.

Each of the first three conditions further implies that

$$(*) \quad r \geq 5 \text{ or } (r = 4 \text{ and } \varepsilon \leq \frac{4}{3} \leq \frac{3}{2}) \text{ or } (r = 3 \text{ and } \varepsilon \leq \frac{3}{5} \leq \frac{3}{4})$$

In the three cases, lemma 3.4 (applied with $N = \deg(T_0 T'_0) \geq 4$) yields a contradiction to $r_{T_0 T'_0} = r$.

Suppose as in (d) that F is of genus 0. Then $F/\mathbb{C}(T)$ is one of the exceptional extensions described in §3.3. But then so is $F'/\mathbb{C}(T)$ as it has the same invariants G , r , \mathbf{C} , and again from §3.3, it must be isomorphic to $F/\mathbb{C}(T)$, a contradiction.

For the second part of theorem 2.1 (b), fix a group $G \in \mathcal{G}^*$. If G is not a subgroup of $\mathrm{PGL}_2(\mathbb{C})$, all Galois extensions $L/\mathbb{C}(T)$ of group G are in \mathcal{E}^* and a $\mathbb{C}(U)$ -parametric extension $F/\mathbb{C}(T)$ of group G is the smallest such extension for the order \prec , hence is unique. If G is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$, then G has a $\mathbb{C}(U)$ -parametric extension $F_m/\mathbb{C}(T)$ (corollary 4.2), which is an exceptional genus 0 extension from §3.3. If $F/\mathbb{C}(T)$ is another $\mathbb{C}(U)$ -parametric extension of group G , it follows from $F_m/\mathbb{C}(T) \prec F/\mathbb{C}(T)$ and $F/\mathbb{C}(T) \prec F_m/\mathbb{C}(T)$ that $F/\mathbb{C}(T)$ has the same invariants as $F_m/\mathbb{C}(T)$, and so, as above, the two must be isomorphic.

3.4.3. An example. Here is an example for which we have $(G, r, g, \mathbf{C}) = (G_{T_0}, r_{T_0}, g_{T_0}, \mathbf{C}_{T_0})$ but $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are not isomorphic, and so $N > 1$. We do not know whether an example exists for which $F/\mathbb{C}(T)$ could additionally be shown to be a specialization of $F_{T_0}/\mathbb{C}(T)$ (which would show that the pre-order \prec is not an order).

Take $G = D_{2n}$ with n odd and $F/\mathbb{C}(T)$ a Galois extension of group G with branch points $0, 1, -1, \lambda$ with $\lambda \in \mathbb{C} \setminus \{0, \pm 1\}$ and ramification indices $\mathbf{e} = (2, 2, 2, 2)$; such an extension exists from the RET and the easy construction of a generating set of G of four elements g_1, \dots, g_4 of order 2 and such that $g_1 \cdots g_4 = 1$.

Take $T_0(U) = U^2/(2U^2 - 2U + 1)$. One checks that $T_0(u) = 0$ has a double root, $u = 0$, and that $T_0(u) = 1$ has a double root, $u = 1$. It follows that both $T_0(u) = -1$ and $T_0(u) = \lambda$ have two distinct roots (because of inequality (2) of the proof of theorem 3.1). From the analysis of the ramification in specialized extensions in the proof of theorem 3.1 (more particularly from (*) and (**)), we obtain that $F_{T_0}/\mathbb{C}(T)$ has $r_{T_0} = 4$ branch points, with ramification indices 2.

The extensions $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are not isomorphic. Otherwise the cross-ratio of their branch points would be equal, up to the sign. The cross-ratio of $0, 1, -1, \lambda$ is $(\lambda - 1)/(2\lambda)$. The branch points of $F_{T_0}/\mathbb{C}(T)$ are the simple roots of $T_0(u) = 1$ and $T_0(u) = \lambda$. Take for example $\lambda = 1/5$. These four points are then $(1 \pm \sqrt{-2})/3$, -1 and $1/3$. A final computation shows the corresponding cross-ratio is $(16 + 4\sqrt{-2})/9$ while $(\lambda - 1)/(2\lambda) = -2$.

Assume $G_{T_0} \neq G$. From theorem 3.1 (a), there exists a sub-extension $L/\mathbb{C}(T)$ of $F/\mathbb{C}(T)$ such that $L \neq \mathbb{C}(T)$, $L_{T_0} = \mathbb{C}(T)$ and L of genus 0. Write $L = \mathbb{C}(\theta)$ for some $\theta \in F$ and $T = A(\theta)/B(\theta)$ with $A, B \in \mathbb{C}[X]$ relatively prime, $B \neq 0$. The irreducible polynomial of θ over $\mathbb{C}(T)$ is $A(Y) - TB(Y)$. Then $L_{T_0} = \mathbb{C}(U)$ means that $A(Y) - T_0(U)B(Y)$ has a root $Y_0(U) \in \mathbb{C}(U)$. But then we have $T_0(U) = A(Y_0(U))/B(Y_0(U))$. As we explain in the last paragraph, T_0 is indecomposable so necessarily $A/B = T_0$ and so L does not depend on λ . The next paragraph provides a contradiction by showing that L is ramified over λ .

The Galois group $\text{Gal}(F/L)$ cannot be a subgroup of the cyclic subgroup of order n of D_{2n} : otherwise, with $d_L = [L : \mathbb{C}(T)]$, the Riemann-Hurwitz formula yields $-2 = -2d_L + 4d_L/2$, a contradiction. Therefore L is the fixed field in F of some involution of D_{2n} . The Riemann-Hurwitz formula gives: $-2 = -2n + R$ where R is the number of ramified primes. Conclude that above each of $0, 1, -1, \lambda$, the number of ramified points is the maximum possible: $(n-1)/2$.

That T_0 is indecomposable is an exercise for which we only indicate the main steps. Deduce from $T_0(U) = A(Y_0(U))/B(Y_0(U))$ that $A(Y_0(U)) = K(U)U^2$ and $B(Y_0(U)) = K(U)(2U^2 - 2U + 1)$ for some $K \in \mathbb{C}(U)$. Writing $Y_0(U) = \alpha(U)/\beta(U)$ with $\alpha, \beta \in \mathbb{C}[U]$ relatively prime, show next that necessarily $Y_0(U) \in \mathbb{C}[U]$ and $K(U) \in \mathbb{C}$. The desired conclusion easily follows.

4. TWISTING REGULAR GALOIS EXTENSIONS IN FAMILIES

Here k -regular extensions $F/k(T)$ are viewed as fundamental group representations, as recalled in §4.1. §4.2 recalls the twisting operation on covers and the twisting lemma (§4.2.1). §4.3 explains how the twisting lemma can be used “in family”. §4.4 states theorem 4.3, which the main result of this section; theorem 2.11 is a special case. Theorem 4.3 is proved in §4.5.

4.1. Fundamental groups representations. The absolute Galois group of a field K is denoted by G_K . If E/K is a Galois extension of group G , an epimorphism $\varphi : G_K \rightarrow G$ such that E is the fixed field of $\ker(\varphi)$ in \overline{K} is called a G_K -representation of E/K .

Given a finite subset $\mathbf{t} \subset \mathbb{P}^1(\overline{K})$ invariant under G_K , the K -fundamental group of $\mathbb{P}^1 \setminus \mathbf{t}$ is denoted by $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$; here t denotes a fixed *base point*, which corresponds to choosing an embedding of $K(T)$ in an algebraically closed field Ω . The (geometric) \overline{K} -fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ is defined as the Galois group of the maximal algebraic extension $\Omega_{\mathbf{t}, K}/\overline{K}(T)$ (inside Ω) unramified above $\mathbb{P}^1 \setminus \mathbf{t}$ and

the (arithmetic) K -fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ as the group of the Galois extension $\Omega_{\mathbf{t},k}/K(T)$.

Degree d K -regular extensions $F/K(T)$ (resp. K -regular Galois extensions $F/K(T)$ of group G) with branch points in \mathbf{t} correspond to transitive homomorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow S_d$ (resp. to epimorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_K \rightarrow G$), with the extra regularity condition that the restriction of ϕ to $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_K, t)_{\overline{K}}$ remains transitive (resp. remains onto). These corresponding homomorphisms are called the *fundamental group representations* (or π_1 -representations for short) of the K -regular (resp. K -regular Galois) extension $F/K(T)$.

Each K -rational point $t_0 \in \mathbb{P}^1(K) \setminus \mathbf{t}$ naturally provides a section $\mathbf{s}_{t_0} : G_K \rightarrow \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ to the exact sequence

$$1 \rightarrow \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \rightarrow \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow G_K \rightarrow 1$$

which is uniquely defined up to conjugation by an element in the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$.

If $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow G$ represents a K -regular Galois extension $F/K(T)$, the morphism $\phi \circ \mathbf{s}_{t_0} : G_K \rightarrow G$ is the *specialized representation* of ϕ at t_0 . The fixed field in \overline{K} of $\ker(\phi \circ \mathbf{s}_{t_0})$ is the specialized extension F_{t_0}/K of $F/K(T)$ at t_0 .

4.2. Twisting regular Galois extensions. For this subsection, we refer to [DG12].

4.2.1. The twisting lemma. Fix a field K and a K -regular Galois extension $\mathcal{F}/K(T)$ of group G , also viewed as K -regular Galois cover $f : X \rightarrow \mathbb{P}^1$. Recall how it can be twisted by a Galois extension E/K of group $H \subset G$. Formally this is done in terms of the associated π_1 - and G_K -representations.

Let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow G$ be a π_1 -representation of $\mathcal{F}/K(T)$ and $\varphi : G_K \rightarrow G$ be a G_K -representation of the Galois extension E/K .

Denote the right-regular (resp. left-regular) representation of G by $\delta : G \rightarrow S_d$ (resp. by $\gamma : G \rightarrow S_d$) where $d = |G|$. Consider the map

$$\tilde{\phi}^\varphi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow S_d$$

defined by the following formula, where R is the restriction map $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \rightarrow G_K$ and \times is the multiplication in the symmetric group S_d :

$$(*) \quad \tilde{\phi}^\varphi(\Theta) = \gamma(\phi(\Theta)) \times \delta(\varphi(R(\Theta))^{-1}) \quad (\Theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K).$$

The map $\tilde{\phi}^\varphi$ is a group homomorphism with the same restriction on $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ as ϕ . It is called the *twisted representation* of ϕ by φ .

The associated K -regular extension is denoted by $\tilde{\mathcal{F}}^\varphi/K(T)$ and called the *twisted extension* of $\mathcal{F}/K(T)$ by φ . The field $\tilde{\mathcal{F}}^\varphi$ is the fixed

field in $\Omega_{\mathbf{t},K}$ of the subgroup $\Gamma \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ of all Θ such that $\tilde{\phi}^\varphi(\Theta)$ fixes the neutral element of G ¹⁰. Finally the corresponding K -regular cover, the *twisted cover* of f by φ , is denoted by $\tilde{f}^\varphi : \tilde{X}^\varphi \rightarrow \mathbb{P}^1$.

The following statement is the main property of the twisted cover.

Twisting lemma 4.1. *Let $t_0 \in \mathbb{P}^1(K) \setminus \mathbf{t}$. The specialization representation $\phi \circ \mathbf{s}_{t_0} : G_K \rightarrow G$ is conjugate in G to $\varphi : G_K \rightarrow G$ if and only if there exists $x_0 \in \tilde{X}^\varphi(K)$ such that $\tilde{f}^\varphi(x_0) = t_0$.*

As a first illustration, we prove the following statement, which we have alluded to several times.

Corollary 4.2. *If $F/\mathbb{C}(T)$ is a Galois extension of group G with F of genus 0, then $F/\mathbb{C}(T)$ is $\mathbb{C}(U)$ -parametric.*

Proof. Let $F/\mathbb{C}(T)$ as above and $L/\mathbb{C}(U)$ be a Galois extension of group $H \subset G$. Let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{C}(U)} \rightarrow G$ be a π_1 -representation of $F\mathbb{C}(U)/\mathbb{C}(U)(T)$ and $\varphi : G_{\mathbb{C}(U)} \rightarrow H \subset G$ be a $G_{\mathbb{C}(U)}$ -representation of the Galois extension $L/\mathbb{C}(U)$. Set $\mathcal{F} = F\mathbb{C}(U)$ and consider the twisted extension $\tilde{\mathcal{F}}^\varphi/\mathbb{C}(U)(T)$ and the associated twisted cover $\tilde{X}^\varphi \rightarrow \mathbb{P}^1$. The extension $\mathcal{F}\overline{\mathbb{C}(U)}/\overline{\mathbb{C}(U)}(T)$ and $F\overline{\mathbb{C}(U)}/\overline{\mathbb{C}(U)}(T)$ are $\overline{\mathbb{C}(U)}(T)$ -isomorphic. Consequently \tilde{X}^φ has the same genus as F , that is 0. From Tsen's theorem, \tilde{X}^φ has a $\mathbb{C}(U)$ -rational point and is isomorphic to \mathbb{P}^1 over $\mathbb{C}(U)$. Conclude thanks to lemma 4.1 that $L/\mathbb{C}(U)$ is a $\mathbb{C}(U)$ -specialization of $F/\mathbb{C}(T)$. \square

It is a similar argument that proves that if K is a Pseudo Algebraically Closed field, then every K -regular Galois extension $F/K(T)$ is K -parametric [Dèb99, §3.3.1].

4.3. Twisting in families. Consider the twisted extension $\tilde{\mathcal{F}}^\varphi/K(T)$ when $K = k(U)$ with k a field and U some indeterminate.

4.3.1. Description of the twisted extension. Every element Θ in the K -fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ uniquely writes $\Theta = \chi \mathbf{s}_U(\sigma)$ with $\chi \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ and $\sigma \in G_K$. Whence

$$\begin{cases} \phi(\Theta) = \phi(\chi) \phi(\mathbf{s}_U(\sigma)) \\ \varphi(R(\Theta)) = \varphi(\sigma) \end{cases}$$

and the following formula, where, by $\text{conj}(g)$ ($g \in G$), we denote the permutation of G induced by the conjugation $x \rightarrow gxg^{-1}$:

$$\tilde{\phi}^\varphi(\Theta) = \gamma(\phi(\chi) \phi(\mathbf{s}_U(\sigma)) \varphi(\sigma)^{-1}) \times \text{conj}(\varphi(\sigma)).$$

¹⁰Taking any other element of G gives the same field up to $K(T)$ -isomorphism.

Conclude that the field $\tilde{\mathcal{F}}^\varphi$ is the fixed field in $\Omega_{\mathbf{t},K}$ of the following subgroup $\Gamma \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$:

$$\Gamma = \{\chi_{\mathbf{s}_U}(\sigma) \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \mid \phi(\chi) = \varphi(\sigma)\phi(\mathbf{s}_U(\sigma))^{-1}\}$$

4.3.2. *The fiber-twisted cover at u_0 .* The two extensions $\mathcal{F}/K(T)$ and $\tilde{\mathcal{F}}^\varphi/K(T)$ are K -regular. From the Grothendieck good reduction theorem, for every $u_0 \in k$ but in a finite subset \mathcal{E} , they specialize at $U = u_0$ to respective extensions $\mathcal{F}|_{u_0}/k(T)$ and $(\tilde{\mathcal{F}}^\varphi)|_{u_0}/k(T)$ that are k -regular of degree

$$[\tilde{\mathcal{F}}^\varphi : k(U)(T)] = [\mathcal{F} : K(T)] = d,$$

have branch point set \mathbf{t}_{u_0} and have the same genus as the common genus of the function fields \mathcal{F} and $\tilde{\mathcal{F}}^\varphi$.

Using the embedding of $\overline{k(U)}$ in the field of Puiseux series in $U - u_0$ and coefficients in \overline{k} , we have a natural monomorphism

$$\mathbf{s}_{u_0} : G_k \rightarrow G_K$$

The morphism $\varphi \circ \mathbf{s}_{u_0} : G_k \rightarrow G$ is well-defined and so is the twisted extension

$$\widetilde{(\mathcal{F}|_{u_0})}^{\varphi \circ \mathbf{s}_{u_0}} / k(T)$$

We call it the *fiber-twisted extension* at u_0 . If $\phi|_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \rightarrow G$ is a π_1 -representation of the k -regular Galois extension $\mathcal{F}|_{u_0}/k(T)$, then a π_1 -representation of the twisted extension above is

$$\widetilde{\phi|_{u_0}}^{\varphi \circ \mathbf{s}_{u_0}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \rightarrow S_d$$

Every element $\theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$ uniquely writes $\theta = x \mathbf{s}_{u_0}(\tau)$ with $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$ and $\tau \in G_k$. Similarly as in §4.3.1 we obtain:

$$\widetilde{\phi|_{u_0}}^{\varphi \circ \mathbf{s}_{u_0}}(\theta) = \gamma(\phi|_{u_0}(x)\phi|_{u_0}(\mathbf{s}_{u_0}(\tau))\varphi(\mathbf{s}_{u_0}(\tau))^{-1}) \times \text{conj}(\varphi(\mathbf{s}_{u_0}(\tau)))$$

The field $\widetilde{(\mathcal{F}|_{u_0})}^{\varphi \circ \mathbf{s}_{u_0}}$ is the fixed field in $\Omega_{\mathbf{t}_{u_0},k}$ of the following subgroup Γ_{u_0} of $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k$:

$$\Gamma_{u_0} = \{x \mathbf{s}_{u_0}(\tau) \mid \phi|_{u_0}(x) = \varphi(\mathbf{s}_{u_0}(\tau))\phi|_{u_0}(\mathbf{s}_{u_0}(\tau))^{-1}\}$$

4.4. Comparison statement.

Theorem 4.3. *For all but finitely many $u_0 \in k$, the two extensions*

$$(\tilde{\mathcal{F}}^\varphi)|_{u_0}/k(T) \text{ and } \widetilde{(\mathcal{F}|_{u_0})}^{\varphi \circ \mathbf{s}_{u_0}}/k(T)$$

are well-defined and are $k(T)$ -isomorphic.

Corollary 4.4. *Let $\tilde{P}^\varphi \in k[U, T, Y]$ be an affine equation of $\tilde{\mathcal{F}}^\varphi/K(T)$. For all but finitely many $u_0 \in k$, the polynomial*

$$\tilde{P}^\varphi(u_0, T, Y)$$

is an affine equation of the k -regular extension $\widetilde{(\mathcal{F}|_{u_0})}^{\varphi \circ s_{u_0}}/k(T)$. Consequently, for all but finitely many $u_0 \in k$ and for all $t_0 \notin (\mathbf{t}|_{u_0} \cup \{\infty\})$, we have this criterion

(*) *there exists $y_0 \in k$ such that $\tilde{P}^\varphi(u_0, t_0, y_0) = 0$ if and only if the specialization representation $\phi|_{u_0} \circ s_{t_0}$ is conjugate in G to $\varphi \circ s_{u_0}$.*

Proof of theorem 2.11. Theorem 2.11 is a special case of corollary 4.4. Namely, from the two k -regular Galois extensions $F/k(T)$ and $L/k(T)$ given in theorem 2.11, consider the K -regular extension $\mathcal{F}/K(T)$ deduced from $F/k(T)$ by scalar extension from k to $K = k(U)$, and let $\varphi : G_K \rightarrow G$ be a G_K -representation of the extension obtained by specializing $LK/K(T)$ at $T = U \in K$. Corollary 4.4 applied for this $\mathcal{F}/K(T)$ and this $\varphi : G_K \rightarrow G$ yields theorem 2.11.

Furthermore, because $\mathcal{F}/K(T)$ is obtained by scalar extension from an extension of $k(T)$, the set \mathcal{E} of bad u_0 in k is a finite subset of k .

Finally the appearance of several polynomials $\tilde{P}_1, \dots, \tilde{P}_n$ in theorem 2.11 comes the fact that its statement is phrased in terms of field extensions rather than in group representations. In the generality of corollary 4.4, we have

(***) *the field extension $E|_{u_0}/k$ is the specialization of $\mathcal{F}|_{u_0}/k(T)$ at t_0 if and only if there exists $\chi \in \text{Aut}(G)$ such that $\phi|_{u_0} \circ s_{t_0}$ is conjugate in G to $\chi \circ \varphi \circ s_{u_0}$.*

and so $\tilde{P}_1, \dots, \tilde{P}_n$ are the polynomials $\tilde{P}^{\chi \circ \varphi}$ with $\chi \in \text{Aut}(G)$. \square

4.5. Proof of theorem 4.3. Let \mathcal{E} be the finite subset given by the Grothendieck good reduction theorem (§5). Fix $u_0 \in k \setminus \mathcal{E}$. The two extensions from the statement of theorem 4.3 are well-defined and have the same branch point set, namely \mathbf{t}_{u_0} . We will show that they are $k(T)$ -isomorphic by showing that they have the same π_1 -representations. We need to compare $\widetilde{\phi|_{u_0}}^{\varphi \circ s_{u_0}}$ from §4.3.2 and some π_1 -representation, say

$$\tilde{\phi}^\varphi|_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \rightarrow S_d$$

of the k -regular extension $(\tilde{\mathcal{F}}^\varphi)|_{u_0}/k(T)$.

As a first step, consider the restrictions of these π_1 -representations to the geometric fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_{\bar{k}}$. Recall that from

the addendum to the Grothendieck good reduction theorem (§5), we have a specialization isomorphism

$$\mathrm{sp}_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \rightarrow \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_{\overline{k}}$$

and that for all $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$, we have

$$\begin{cases} \phi|_{u_0}(x) = \phi \circ \mathrm{sp}_{u_0}^{-1}(x) \\ \widetilde{\phi}^\varphi|_{u_0}(x) = \widetilde{\phi}^\varphi \circ \mathrm{sp}_{u_0}^{-1}(x) \end{cases}$$

Using §4.3.1, we obtain

$$\widetilde{\phi}^\varphi|_{u_0}(x) = \gamma(\phi(\mathrm{sp}_{u_0}^{-1}(x))) = \gamma(\phi|_{u_0}(x)) = \widetilde{\phi|_{u_0}}^{\varphi \circ \mathbf{s}_{u_0}}(x)$$

To compare the restrictions to G_k of the two π_1 -representations, first show the following.

Lemma 4.5. *For all but finitely many $u_0 \in k$ and all $\tau \in G_k$, we have*

$$\phi|_{u_0}(\mathbf{s}_{u_0}(\tau)) = \phi(\mathbf{s}_U \circ \mathbf{s}_{u_0}(\tau))$$

Proof. Namely, with \mathcal{Y}_1 a primitive element of $\mathcal{F}/K(T)$, which we may assume to be integral over $k[U, T]$, the right-hand side term corresponds to the action of $\mathbf{s}_{u_0}(\tau) \in G_K$ on the d different K -conjugates

$$\mathcal{Y}_i = \sum_{n=0}^{\infty} b_{in}(U)(T - U)^n, \quad j = 1, \dots, d$$

of \mathcal{Y}_1 , viewed in $\overline{K}((T - U))$; the action of $\mathbf{s}_{u_0}(\tau)$ is given by the action on the coefficients $b_{in}(U) \in \overline{K}$ ($n \geq 0$).

From the Eisenstein theorem, there exists a polynomial $E(U) \in k[U]$, $E(U) \neq 0$, such that $E(U)^{n+1} b_{in}(U) \in k[U]$ for every $n \geq 0$, $i = 1, \dots, d$. Enlarge again the set \mathcal{E} to contain the roots of $E(U)$. Then $\mathcal{Y}_1, \dots, \mathcal{Y}_d$ can be specialized at $U = u_0$ to yield d formal power series in $\overline{k}[[T - u_0]]$

$$\mathcal{Y}_i|_{u_0} = \sum_{n=0}^{\infty} b_{in}(u_0)(T - u_0)^n, \quad j = 1, \dots, d$$

If \mathcal{E} is again enlarged to contain the roots of the bad prime divisor of the irreducible polynomial $P \in k[U, T, Y]$ of \mathcal{Y}_1 over $k(U, T)$ (§5), then $P(u_0, T, Y)$ is irreducible in $\overline{k}[T, Y]$; it is the irreducible polynomial of $\mathcal{Y}_1|_{u_0}$ and the extension $k(T, \mathcal{Y}_1|_{u_0})/k(T)$ is $k(T)$ -isomorphic to the extension $\mathcal{F}|_{u_0}/K(T)$.

The left-hand side term $\phi|_{u_0}(\mathbf{s}_{u_0}(\tau))$ of the claimed formula corresponds to the action of $\tau \in G_k$ on the d different K -conjugates $\mathcal{Y}_1|_{u_0}, \dots, \mathcal{Y}_d|_{u_0}$, with τ acting on the coefficients $b_{in}(u_0) \in \overline{k}$ ($n \geq 0$). Clearly we have

$$(\mathbf{s}_{u_0}(\tau)(b_{in}(U)))|_{u_0} = \tau(b_{in}(u_0)), \quad (i = 1, \dots, d, n \geq 0)$$

and so

$$(\mathbf{s}_{u_0}(\tau)(\mathcal{Y}_i)|_{u_0} = \tau(\mathcal{Y}_i|_{u_0}), \quad (i = 1, \dots, d)$$

which corresponds to the claim. \square

Lemma 4.5, applied with $\tilde{\phi}^\varphi$ replacing ϕ also gives

$$\tilde{\phi}^\varphi|_{u_0}(\mathbf{s}_{u_0}(\tau)) = \tilde{\phi}^\varphi(\mathbf{s}_U \circ \mathbf{s}_{u_0}(\tau))$$

Using §4.3.1, we obtain

$$\begin{aligned} \tilde{\phi}^\varphi|_{u_0}(\mathbf{s}_{u_0}(\tau)) &= \gamma(\phi(\mathbf{s}_U \circ \mathbf{s}_{u_0}(\tau)) \delta(\varphi(\mathbf{s}_{u_0}(\tau))) \\ &= \gamma(\phi|_{u_0}(\mathbf{s}_{u_0}(\tau)) \delta(\varphi(\mathbf{s}_{u_0}(\tau))) \\ &= \widetilde{\phi|_{u_0}^{\varphi \circ \mathbf{s}_{u_0}}}(\mathbf{s}_{u_0}(\tau)) \end{aligned}$$

This concludes the proof of $\widetilde{\phi|_{u_0}^{\varphi \circ \mathbf{s}_{u_0}}} = \tilde{\phi}^\varphi|_{u_0}$ and so of theorem 4.3.

5. APPENDIX: GOOD REDUCTION & SPECIALIZATIONS OF COVERS

This appendix recalls some classical results which essentially go back to Grothendieck about the good reduction of K -regular extensions and the inertia in their specializations. We have adjusted to our situation the original statements which hold in a bigger generality; in particular our statements are phrased in field extension terms rather than in a scheme theoretic language.

Assume K is the fraction field of a Dedekind domain A ; typically $K = k(U)$ and $A = k[U]$ with U a new indeterminate.

Given a non-zero prime ideal $\mathfrak{p} \subset A$ (typically $\mathfrak{p} = \langle U - u_0 \rangle$ with $u_0 \in k$ when $A = k[U]$), denote the residue field by $\kappa_{\mathfrak{p}}$, the completion of A (resp. of K) at \mathfrak{p} by $\tilde{A}_{\mathfrak{p}}$ (resp. by $\tilde{K}_{\mathfrak{p}}$), the algebraic closure of $\tilde{K}_{\mathfrak{p}}$ by $C_{\mathfrak{p}}$ and fix an embedding $\overline{K} \subset C_{\mathfrak{p}}$.

Let $F/K(T)$ be a K -regular extension of group G , with branch point set $\mathbf{t} = \{t_1, \dots, t_r\}$, inertia canonical invariant $\mathbf{C} = (C_1, \dots, C_r)$ and associated ramification indices $\mathbf{e} = (e_1, \dots, e_r)$. Let $\mathfrak{p} \subset A$ be a non-zero prime ideal. We recall below some classical results about

- (a) the good reduction of $F/K(T)$ modulo the prime ideal \mathfrak{p} , and,
- (b) the ramification above the prime ideal \mathfrak{p} in specializations F_{t_0}/K at points $t_0 \in \mathbb{P}^1(K)$.

These results go back to general results of Grothendieck [Gro71], [GM71] and more specific versions by Beckmann for regular extensions $F/K(T)$ over number fields [Bec91]. Here, regarding (b), we follow Legrand's variant [Legar, §2] extending Beckmann's statement to the situation the ground field is the fraction field of an arbitrary Dedekind domain. For (a) we follow the variant given in [Dèb16].

Classical assumptions. We first list some classical assumptions involved in these statements; we refer to the articles cited above for more details about them. The main point we will use is that each of them is satisfied for all but finitely many primes \mathfrak{p} .

- (1) $|\mathcal{G}| \notin \mathfrak{p}$
- (2) *there is no vertical ramification at \mathfrak{p} in the extension $F/K(T)$.*
- (3) *no two different branch points of $F/K(T)$ meet modulo \mathfrak{p} .*
- (4) *the ideal \mathfrak{p} is unramified in the extension $K(t_1, \dots, t_r)/K$.*
- (5) *t_i and $1/t_i$ are integral over $\tilde{A}_{\mathfrak{p}}$, $i = 1, \dots, r$.*

We will say that \mathfrak{p} is a *bad prime of the extension $F/K(T)$* if conditions (2), (3) hold¹¹ and that it is *good* otherwise.

We also recall the related notion of *good/bad primes of a non-constant polynomial $P \in A[T, Y]$* , irreducible in $\overline{K}[T, Y]$ and monic in Y , defined in [Dèb16]: a non-zero element $\mathcal{B}_P \in A$ is constructed and called the *bad prime divisor of P* ; it is essentially the discriminant w.r.t T of some “reduced form” of the discriminant $\Delta_P(T)$ of P w.r.t. Y . A prime \mathfrak{p} is said to be a *good prime of P* if

- (6) $\mathcal{B}_P \notin \mathfrak{p}$.

Again there are only finitely many *bad primes* for the polynomial P . The two notions compare as follows: if \mathfrak{p} is good for P then it is also good for the extension $K(T)[Y]/\langle P \rangle$ of $K(T)$.

Let B be the integral closure of $\tilde{A}_{\mathfrak{p}}[T]$ in the field $F\tilde{K}_{\mathfrak{p}}$.

Grothendieck good reduction theorem. *Assume that \mathfrak{p} is a good prime of $F/K(T)$ and that assumption (1) holds. Then the extension $F/K(T)$ has good reduction at \mathfrak{p} , i.e.: $\mathfrak{p}B$ is a prime ideal of B and the fraction field ε of $B/\mathfrak{p}B$ is a separable extension of $\kappa_{\mathfrak{p}}(T)$ and satisfies*

$$[\varepsilon : \kappa_{\mathfrak{p}}(T)] = [\overline{\kappa_{\mathfrak{p}}} \varepsilon : \overline{\kappa_{\mathfrak{p}}}(T)] = [F : K(T)] = \deg_Y(P). \quad ^{12}$$

The extension $\varepsilon/\kappa_{\mathfrak{p}}(T)$ is called the (*good*) *reduction of $F/K(T)$ at \mathfrak{p}* and denoted by $F|_{\mathfrak{p}}/\kappa_{\mathfrak{p}}(T) = F|_{u_0}/k(T)$ when $\mathfrak{p} = \langle U - u_0 \rangle \subset A = k[U]$. The vertical bar in the notation is meant to distinguish the reduction from the specialization. The extension $F|_{\mathfrak{p}}/\kappa_{\mathfrak{p}}(T)$ is $\kappa_{\mathfrak{p}}$ -regular and its branch point set is the reduction, denoted by $\mathfrak{t}_{\mathfrak{p}}$, of the set \mathfrak{t} modulo an (arbitrary) prime ideal above \mathfrak{p} of the integral closure of $A_{\mathfrak{p}}$ in $K_{\mathfrak{p}}(\mathfrak{t})$.

¹¹Legrand also includes (1) and (4). For consistency with the other good/bad prime notion, we prefer to stick to (2) and (3) and repeat (1) and (4) when necessary.

¹²geometrically: if $\tilde{f}_0 : \tilde{\mathcal{C}}_0 \rightarrow \mathbb{P}_{\kappa_{\mathfrak{p}}}^1$ is the special fiber of \tilde{f} , then \tilde{f}_0 is generically étale, $\tilde{\mathcal{C}}_0$ is geometrically irreducible and $[\overline{\kappa_{\mathfrak{p}}}(\tilde{\mathcal{C}}_0) : \overline{\kappa_{\mathfrak{p}}}(T)] = [F : K(T)]$.

When the residue field $\kappa_{\mathfrak{p}}$ is algebraically closed, we have this more precise addendum. Its statement uses the notion of fundamental group representation of an extension $F/\overline{K}(T)$; it is recalled in §4.1.

Addendum to Grothendieck good reduction theorem. *Under the same assumptions, there is a specialization isomorphism*

$$\mathrm{sp}_{\mathfrak{p}} : \pi_1(\mathbb{P}^1 \setminus \mathfrak{t}, t)_{\overline{K}} \rightarrow \pi_1(\mathbb{P}^1 \setminus \mathfrak{t}_{\mathfrak{p}}, t)_{\overline{\kappa_{\mathfrak{p}}}}$$

which has this further property: if $\phi_{\overline{K}} : \pi_1(\mathbb{P}^1 \setminus \mathfrak{t}, t)_{\overline{K}} \rightarrow G \subset S_d$ is a π_1 -representation of the extension $F\overline{K}/\overline{K}(T)$, then the morphism

$$\phi_{\overline{K}} \circ \mathrm{sp}_{\mathfrak{p}}^{-1} : \pi_1(\mathbb{P}^1 \setminus \mathfrak{t}_{\mathfrak{p}}, t)_{\overline{\kappa_{\mathfrak{p}}}} \rightarrow G \subset S_d$$

is a π_1 -representation of the reduction $F|_{u_0}/\kappa_{\mathfrak{p}}(T)$.

Let $P \in A[T, Y]$ be a non-constant polynomial, irreducible in $\overline{K}[T, Y]$, monic in Y , *e.g.* an affine equation of the K -regular extension $F/K(T)$.

Polynomial form of the Grothendieck good reduction theorem

Assume that \mathfrak{p} is a good prime of P and that assumption (1) holds. Then the polynomial “ P modulo \mathfrak{p} ” in $\kappa_{\mathfrak{p}}[T, Y]$ is irreducible in $\overline{\kappa_{\mathfrak{p}}}[T, Y]$ and of group G .

As explained in [Dèb16], this polynomial conclusion is more precise than the field extension conclusion from GRT; the assumption is however also stronger. Finally we recall the conclusions from [Legar] about the inertia in specializations.

Specialization Inertia Theorem. *Let $t_0 \in \mathbb{P}^1(K) \setminus \mathfrak{t}$.*

(a) *If \mathfrak{p} ramifies in F_{t_0}/K , then $F/K(T)$ has vertical ramification at \mathfrak{p} (i.e. condition (2) holds) or t_0 meets some branch point modulo \mathfrak{p} .*

(b) *Assume that \mathfrak{p} is a good prime of $F/K(T)$ and assumptions (1), (4), (5) holds. If for some $i \in \{1, \dots, r\}$, t_0 and t_i meet modulo \mathfrak{p} , then the inertia group of F_{t_0}/K at \mathfrak{p} is conjugate in G to the cyclic group*

$$\langle g_i^{I_{\mathfrak{p}}(t_0, t_i)} \rangle$$

where g_i is any element of the conjugacy class C_i and $I_{\mathfrak{p}}(t_0, t_i)$ is the intersection multiplicity of t_0 and t_i .

REFERENCES

- [Bec91] Sybilla Beckmann. On extensions of number fields obtained by specializing branched coverings. *J. Reine Angew. Math.*, 419:27–53, 1991.
- [BR97] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Compositio Math.*, 106(2):159–179, 1997.
- [CS82] J. W. S. Cassels and A. Schinzel. Selmer’s conjecture and families of elliptic curves. *Bull. London Math. Soc.*, 14(4):345–348, 1982.

- [CT00] Jean-Louis Colliot-Thélène. Rational connectedness and Galois covers of the projective line. *Ann. of Math. (2)*, 151(1):359–373, 2000.
- [DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30:303–338, 1997.
- [Dèb99] Pierre Dèbes. Galois covers with prescribed fibers: the Beckmann-Black problem. *Ann. Scuola Norm. Sup. Pisa*, Cl. Sci. (4), 28:273–286, 1999.
- [Dèb16] Pierre Dèbes. Reduction and specialization of polynomials. *Acta Arith.*, 172.2:175–197, 2016.
- [Dèbar] Pierre Dèbes. On the Malle conjecture and the self-twisted cover. *Israel J. Math.*, to appear.
- [DG12] Pierre Dèbes and Nour Ghazi. Galois covers and the Hilbert-Grunwald property. *Ann. Inst. Fourier*, 62/3:989–1013, 2012.
- [DL13] Pierre Dèbes and François Legrand. Specialization results in Galois theory. *Trans. Amer. Math. Soc.*, 365(10):5259–5275, 2013.
- [FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. (second edition).
- [GM71] Alexandre Grothendieck and Jacob P. Murre. *The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme*, volume 208 of *LMN*. Springer, 1971.
- [GMPS15] Simon Guest, Joy Morris, Cheryl E. Praeger, and Pablo Spiga. On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.*, 367(11):7665–7694, 2015.
- [Gro71] Alexandre Grothendieck. *Revêtements étales et groupe fondamental*, volume 224 of *LMN*. Springer, 1971.
- [HM99] Ki-Ichiro Hashimoto and Katsuya Miyake. Inverse Galois problem for dihedral groups. In *Number theory and its applications (Kyoto, 1997)*, volume 2 of *Dev. Math.*, pages 165–181. Kluwer Acad. Publ., Dordrecht, 1999.
- [JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials. Constructive Aspects of the Inverse Galois Problem*. Cambridge University Press, 2002.
- [Leg13] François Legrand. Spécialisations de revêtements et théorie inverse de Galois. *PhD thesis - Université Lille 1*, 2013.
- [Leg15] François Legrand. Parametric Galois extensions. *J. Algebra*, 422:187–222, 2015.
- [Leg16a] François Legrand. On parametric extensions over number fields. *preprint*, 2016. arXiv:1602.06706.
- [Leg16b] François Legrand. Twists of super elliptic curves without rational points. *preprint*, 2016.
- [Legar] François Legrand. Specialization results and ramification conditions. *Isr. J. Math.*, (to appear). arXiv:1310.2189.
- [Sch82] Andrzej Schinzel. *Selected topics on polynomials*. University of Michigan Press, Ann Arbor, Mich., 1982.
- [Sch00] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

- [Sel54] Ernst S. Selmer. A conjecture concerning rational points on cubic curves. *Math. Scand.*, 2:49–54, 1954.
- [Ser92] Jean-Pierre Serre. *Topics in Galois Theory*. Research Notes in Mathematics. Jones and Bartlett Publishers, 1992.
- [Tho84] John G. Thompson. Some finite groups which appear as $\text{Gal } L/K$, where $K \subseteq \mathbf{Q}(\mu_n)$. *J. Algebra*, 89(2):437–499, 1984.

E-mail address: `Pierre.Debes@math.univ-lille1.fr`

LABORATOIRE PAUL PAINLEVÉ, MATHÉMATIQUES, UNIVERSITÉ LILLE 1, 59655
VILLENEUVE D’ASCQ CEDEX, FRANCE